UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA, Plaintiff,	)	No. 2:11-cr-00070-RAJ
vs.	)	Seattle, WA
ROMAN V. SELEZNEV, Defendant.	)	Jury Trial, Day 5 August 19, 2016

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE JUDGE RICHARD A. JONES
UNITED STATES DISTRICT COURT

APPEARANCES:

FOR THE PLAINTIFF:

NORMAN McINTOSH BARBOSA
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
norman.barbosa@usdoj.gov

C. SETH WILKINSON
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
seth.wilkinson@usdoj.gov

HAROLD W. CHUN
U.S. Department of Justice
1301 New York Avenue NW, Suite 600
Washington, DC 20005
harold.chun@usdoj.gov

FOR THE DEFENDANT: JOHN HENRY BROWNE
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
johnhenry@jhblawyer.com

EMMA SCANLAN
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
emma@jhblawyer.com

Andrea Ramirez, CRR, RPR
Official Court Reporter
United States District Court
Western District of Washington
700 Stewart Street, Suite 17205
Seattle, WA 98101
andrea_ramirez@wawd.uscourts.gov

Reported by stenotype, transcribed by computer

I N D E X

E X H I B I T S

THE CLERK: We are resuming our jury trial in the matter of the United States vs. Roman Seleznev, Cause Number CR11-70, assigned to this court.

THE COURT: Before we begin, Juror Number 15, would you like to move to the regular seat?

JUROR: No, thank you, sir.

THE COURT: Are you comfortable there?

JUROR: Yes, I am.

THE COURT: Okay. If you decide to change, and you want to move around, let me know.

JUROR: Okay.

THE COURT: Counsel, please call your witness back to the stand.

MR. BARBOSA: The government calls Richard Noel.

THE COURT: Ladies and gentlemen of the jury, you'll recognize that we haven't completed the testimony of the last witness who was testifying on behalf of the government. It's often the case, to accommodate witnesses, that we will have witnesses interrupted so that we can accommodate another witness, and that's what we're doing now. As soon as this witness -- or when the government finishes the witnesses that need to testify, we'll go back and resume with the other witness's testimony. So if you need to adjust your notes, please do so accordingly.

Counsel?

MR. BARBOSA: Thank you, Your Honor.

THE CLERK: Please raise your right hand.

RICHARD NOEL, having been duly sworn, was examined and testified as follows:

THE CLERK: If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Richard Noel, N-O-E-L.

DIRECT EXAMINATION

BY MR. BARBOSA

Q Good morning, Mr. Noel.

A Good morning.

Q Could you tell the jurors where you work?

A I work with the Federal Deposit Insurance Corporation, in Seattle.

Q What is the Federal Deposit Insurance Corporation?

A The FDIC, our mission is to insure financial institutions throughout the United States. And we also participate in the regulatory process of those institutions.

Q Is the FDIC a federal agency?

A We are.

Q How long have you worked for the FDIC?

A Thirty years.

Q And what are your duties with the FDIC?

A I'm a risk examiner. So as a part of that, I'm involved in the examination process in the institutions that we're

responsible for.
Q And are you stationed here in Seattle?
A I am, yes.
Q What institutions are you responsible for, here in the Seattle area? Or what is your geographic jurisdiction?
A Washington state and then also Alaska.
Q Okay. Are you also familiar with FDIC's practices nationwide, as part of your work?
A Yes. Generally, yes.
Q What does it mean to review the risk practices of the banks in your jurisdiction?
A So we assess the risk of an institution by reviewing their credit, their lending, and their operation practices within an institution.
Q And why does the FDIC do that?
A Well, we're a federal agency. We're responsible for insuring the deposits of the financial institution, so that's one of our primary responsibilities.
Q Does examining the lending practices of the institutions include their credit card lending practices?
A Yes, it would.
Q Why?
A Well, it is a lending product, and it also potentially represents risk to the institution. So any lending product, or any operational risk in an institution, we would be responsible

for reviewing and assessing the risk of.
Q Were you asked to review FDIC's records to determine if a number of specific banks in this case were insured between 2007 and 2014?
A Yes, I was.
Q Do you recall which banks those included?
A I do recall the banks.
Q Which ones were they?
A Capital One, HSBC, U.S. Bank, Citibank, Wells Fargo, FIA.
Q Was Chase one of those banks?
A And JPMorgan Chase.
Q Okay. Let's start with FIA.
Is FIA Card Services the full name of that bank?
A That is correct.
Q What did you determine -- did you review FDIC's records related to FIA Card Services?
A I did.
Q And what did you look at the records for?
A I looked for the insured status of that institution, the insured -- actual insured date. And I also looked to make sure there was no lapses in the FDI insurance for that institution.
Q And what did you find?
A I found that there were no lapses, and I found that the insured date of that institution was January 1991.
Q And did their deposits remain insured through the present

time?
A They did.
Q Was FIA Card Services previously known by another name?
A It was.
Q What was that?
A MSNB, I believe.
Q Are you familiar with a bank known as MBNA?
A Correct.
Q Was that possibly the name?
A Yes.
Q Turning to HSBC Bank, did you review FDIC records for that bank?
A I did.
Q What did you learn about --

MS. SCANLAN: Your Honor, I'm going to object that at this point the witness has not established the foundation for the records that he's testifying about.

THE COURT: Let's clarify, Counsel.

BY MR. BARBOSA
Q What type of records did you review to examine the insured status of the institutions?
A I reviewed our system of records that we have within the FDIC.
Q What do those system of records tell you about insured status in the history of an institution?

A Well, it indicates what the actual insured date was for the institution. It also gives a transaction of the status of the institution, throughout the history of the institution, if there were any changes in name or relocation of that institution.

Q And does FDIC rely on those records to establish whether an institution is or is not insured at any given time?

A We would, yes.

Q So turning back to HSBC Bank, did you review the records specific to that bank?

A I did.

Q What did you learn about their insured status?

A The insured status was in place, and the actual insured date of that institution was July 19 -- excuse me -- July 2004.

Q How long have they remained insured?

A They have remained insured since their inception of their actual insured date.

Q Through the present time?

A Yes.

Q What about Citibank National Association Bank?

A I did review the records for that bank. The insured date for that institution was January 1934.

Q And have they remained insured through the present time?

A Yes, they have.

Q Have they gone through a number of name changes throughout

their history?
A They have, yes, since the beginning of the institution, which dates back to the 19th century.
Q Did you review the insured status of Wells Fargo Bank?
A I did.
Q What did you learn about their history of insured status with the FDIC?
A The insured date for that institution was January 1934. That institution has remained insured throughout -- until 2014.
Q That was the same as Citibank, it sounds like.
When was FDIC founded and created?
A FDIC was founded in 1933. The actual insurance of the institutions began in January, as of January 1, 1934.
Q So have those two institution been insured for the entire time period of the FDIC's existence?
A Yes.
Q Did you review the insured status for Capital One Bank?
A I did.
Q What did you learn about their insured status?
A That institution was insured as of November 1994.
Q And did they remain insured through the present date?
A They have.
Q What about U.S. Bank National Association?
A U.S. Bank was insured as of January 1, 1934.
Q And how long did they remain insured?

A They have remained insured throughout the history of the the institution.
Q Through the present date?
A Yes.
Q And finally, JPMorgan Chase Bank National Association, did you look at their insured status?
A I did.
Q What did you learn about theirs?
A JPMorgan Chase was insured as of January 1, 1934. They have remained insured throughout the history of the institution, to the current time.
Q These banks, how do they fit into FDIC's regulatory scheme?
A Well, these are large institutions. We do participate in the regulatory process for these institutions. We are not the primary federal regulator for them, but we do participate. We have backup authority that we can exercise, if necessary. Typically, what we would have is a resident examiner, or examiners, that participate in the examination process for these institutions.
Q Does FDIC also insure smaller banks?
A We do.
Q Do banks -- in your experience, do banks in the U.S. typically operate without FDIC insurance?
A No.

Q Why not?
A Well, there is no federal law or mandate that requires an institution to have deposit insurance, but the reputation at risk for those institutions would be to the extent that they really couldn't operate very long.
Q In your experience, have you come across banks that were operating without FDIC insurance?
A I have not.
Q And how many banks have you, approximately, examined during the course of your employment?
A I would guess in the range of approximately 100.

MR. BARBOSA: No further questions, Your Honor.

THE COURT: Cross examination?

MS. SCANLAN: I have no questions, Your Honor.

THE COURT: Any objection to this witness being excused, by the government?

MR. BARBOSA: None from the government, Your Honor.

THE COURT: From the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you, sir. You may step down.

Next witness, Counsel?

MR. BARBOSA: The government calls Jason Winship.

THE COURT: Please step forward, sir.

THE CLERK: Please raise your right hand, before you're seated.

JASON WINSHIP, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Jason Winship, last name spelled W-I-N-S-H-I-P.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MR. BARBOSA

Q Good morning, Mr. Winship.

Could you tell the jurors where you work?

A I work at the National Credit Union Administration.

Q What is the National Credit Union Administration?

A We're an agency of the federal government that regulates and insures the majority of the credit unions in the nation.

Q What type of regulatory responsibilities does the NCUA have for credit unions?

A The regulatory responsibility would be -- well, we provide them with share insurance, and we conduct safety and soundness examinations to ensure integrity of the insurance fund.

Q How long have you worked for the NCUA?

A Twenty years.

Q What are your duties with the NCUA?

A Currently, I'm a supervisor examiner. I supervise a group

of safety and soundness examiners.

Q What is a safety and soundness exam?

A We conduct annual examinations of federally insured credit unions. And that entails reviewing the books and records, internal controls, you know, policies, loan files, interest rate risk, basically all the risk to the credit union. We assess management's ability to safeguard the assets of the credit union.

Q Does that include credit card lending practices?

A Yes, it would.

Q Why does the NCUA examine the risks to the credit unions that it insures?

A Basically to safeguard the insurance fund, make sure the credit unions do not fail due to mismanagement, taking on too much risk.

Q Were you asked to review NCUA records to determine if a number of credit unions in this case were insured between 2007 and 2014?

A Yes.

Q What type of records did you review?

A I reviewed our database, our central database, kept in Alexandria, Virginia; management information systems, basically. We call it "MIS." That includes all of the records of the credit unions, active and inactive.

Q Does that record system tell you when and how long the

credit union has been insured by the NCUA?
A Yes, it does.
Q And do you rely on those records, and does the NCUA rely on those records to determine insured status for particular credit unions?
A Yes.
Q I'd like to draw your attention to a few particular credit unions.
Did you review the NCUA's records related to the Boeing Employees Credit Union?
A Yes, I did.
Q What did you find in terms of their insured status and when they became insured?
A BECU, or Boeing, was first insured in 1975.
Q Did they continue to remain insured through the present day?
A Yes.
Q Did you review records for Alaska USA Federal Credit Union?
A Yes, I did.
Q What did you learn about their insured status?
A They were first insured in 1971.
Q How long did they remain insured?
A They are still insured today.
Q Did you review records for Navy Federal Credit Union?

A Yes.
Q What did you learn about their insured status?
A They were insured in 1971.
Q They remain insured through the present day?
A Yes.
Q What about Washington State Employees Credit Union?
A They were insured in 1971, and remain insured today.
Q And Seattle Metropolitan Credit Union?
A They attained federal insurance in 1997, and remain insured today.
Q Are some of those credit unions local credit unions that are under your jurisdiction?
A Yes, they are.
Q Are others part of a different system, or regulated differently?
A Navy Federal Credit Union is headquartered in Alexandria, Virginia. But they have branch offices around the country, around the world.
Q Approximately how many credit unions do you have supervising examining authority over in your jurisdiction?
A I have approximately 60.
Q In Washington state, are you aware of credit unions that operate without national credit union insurance?
A No, not in Washington state.
Q Why wouldn't there be?

A The private insurer, I believe, was Washuga (phonetic). This is going back to when I just began with NCUA. It went under, basically due to credit union losses. And this is possibly '96/'97 when this happened. That kind of correlates with Seattle Metropolitan's federal insurance date of '97. They were one of the credit unions that was privately insured. And due to that failure of that private insurer, the State of Washington passed a law that any credit union operating in the state of Washington had to have federal insurance.

MR. BARBOSA: No further questions, Your Honor.

THE COURT: Cross examination?

MS. SCANLAN: No questions, Your Honor.

THE COURT: Any objection to this witness being excused, by the government?

MR. BARBOSA: No, Your Honor. Thank you.

THE COURT: By the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you, sir. You may step down. You're excused.

Counsel, next witness?

MR. WILKINSON: The United States calls Special Agent Keith Wojcieszek.

THE COURT: Please have him step forward.

Please step forward, sir.

THE CLERK: Please raise your right hand.

KEITH WOJCIESZEK, having been duly sworn, was examined and testified as follows:

THE CLERK: Please have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Certainly. It's Keith Wojcieszek, spelled W-O-J-C-I-E-S-Z-E-K.

THE COURT: You may inquire.

MR. WILKINSON: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. WILKINSON

Q Good morning, Special Agent.

A Good morning, sir.

Q Where are you employed?

A I'm employed with the U.S. Secret Service.

Q How long have you been employed by the U.S. Secret Service?

A Just about 14-and-a-half years.

Q Where did you begin your employment there?

A I was a uniformed officer for a couple years, and then I got hired by the agent side, in 2004.

Q Okay. And where did you -- where was your first post, starting in 2004?

A In 2004, I was assigned to the Louisville Field Office, in Louisville, Kentucky.

Q And were you a member of any particular task force there?
A Yes. I was a member of the Electronic Crimes Task Force. I was the forensic examiner at that task force, in the office.
Q What kind of crimes were you examining there?
A Electronic crimes.
Q And how long did you stay with the Louisville Electronic Crimes Task Force?
A Approximately six years.
Q And where did you go after that?
A I went to our headquarters, to the cyber intelligence section.
Q And when was that?
A That was May of 2010.
Q How long did you stay there?
A I was there for two years.
Q And what did you do after that?
A After that, I was assigned to our counterassault team, which is kind of like a SWAT team in the Secret Service, for the President's detail. I was there for about three-and-a-half years.
Q What's the function of the counterassault team?
A We would do the tactical entities of any kind of travel for the President, Vice President, any high-level risk targets that would come to the United States.
Q And what is your current position?

A I'm assigned to the presidential detail of President Obama, the transportation section, or driving the limos, pretty much; put it that way.

Q I want to focus on your period of employment between May 2010 and May 2012.

Is that the time you said you were assigned to the cyber intelligence section?

A That's correct, sir, yes.

Q And we heard yesterday from Special Agent Szydlik.

Is that the same section where he worked?

A Yes, sir.

Q And can you remind us what the mission of that part of the Secret Service is?

A The mission of that part is kind of concentrating on computer crimes, electronic crimes, anything of a large scale. We try to focus on -- in our headquarters assignment more on outside the United States, worldwide crime, just because we have the assets, the entities within the headquarters, in D.C.

Q So what did you do on a daily basis in pursuit of that?

A I did multiple things. Initially, I started off as an undercover agent, as you would say, online. I would go into different forums, kind of look through and just see, you know, what's going on in the criminal world on these forums.

Q And let me just stop you there.

When you say "forums," do you mean carding forums?

A Yes; carding forums that would sell credit cards, that would sell personal information, that would sell malware, anything that someone could use to highjack financial infrastructure. Because the Secret Service is responsible for the financial infrastructure of the United States.

So on a daily basis, I would be on these forums to see what's, kind of, trending. On top of that, I would talk to individuals, either other law enforcement, or some criminals that are online that I was posed as another criminal. And then I would, on top of that, do just investigative stuff. I would go and serve subpoenas -- I'm sorry -- request subpoenas, search warrants, collect any kind of electronic evidence that I can go through and comb and see; kind of compare what other servers throughout the world would have with what I'm investigating. So we'd log all this information into our database, and kind of search through that.

Q Were there any particular carding forums that you focused on during your time with the cyber investigative section?

A Yes, there were several. But the most prominent one, that had the most members, that we had an account for, was carder.su. It changed its name. If you type it on the HTML website, it would change its name. But the last time, it was C-R-D-R, dot, S-U. I would log into there and kind of comb through there, and see what was going on in that forum.

Q What does the "su" stand for?

A Soviet Union.
Q What types of items or topic areas were discussed on the carder.su forum?
A There were several. They varied from botnets, which basically someone else is controlling your computer, to skimming cards. Either you want to purchase a skimmer or -- I don't know if you're familiar with what a skimmer is. A skimmer is if -- just, for example, when you swipe your card through anything, even through a door lock, or something like that, it reads the data. The black on the back of your credit card, it has the data there. And people can sell that, so they can re-encode it to anything, anything that has a magnetic strip. You can re-encode any information. So you can gather stuff like that. There's selling of actual credit card numbers; whereas if someone were to steal your credit card information, you can go on there, and you can talk about, "Hey, I'm looking for this. Can you help me out? I'm looking for credit cards," to looking at personal information. You could buy fake IDs. You could do just a multiple of different things on this website.
Q Could anyone just go onto the carder.su website and converse, or did you have to be a member?
A No. You had to be a member. And there were two different --
MS. SCANLAN: Objection. I think he already answered

the question.

MR. WILKINSON: I'll ask another question.

THE COURT: That's fine, Counsel.

BY MR. WILKINSON

Q Were there different ways that a person could become a member on carder.su?

A Yes. There are kind of two distinct ways you could do it. Either one, you could pay a small fee. So if someone wanted to go on, you pay a small fee. And I can't recall the exact fee. It's, like, a hundred dollars or so. But the majority of people that pay the fee would be law enforcement, because they just want to get on and view.

Then there's another way. You have approximately 25,000 different members on this. It's one of the larger forums. So if the administrator, who kind of maintains all the information on there, would have another member verify, "Hey, this guy is a good guy. He's not a cop. He's all right. Let him on the forum," that guy is putting up his identity to the new identity to kind of recommend him. That's another way you can get on these forums.

Q Were you able to obtain a membership to the carder.su forum?

A I was, yes.

Q And how did you get that membership?

A One of the individuals that we arrested gave us consent to

go ahead and use his identity on the website.

Q So did you spend -- let me back up.

How many times do you think you visited the carder.su forum?

A Two years, I was probably on there at least once or twice every day. I was on there every day.

Q You mentioned the forum had about 25,000 members?

A Give or take a thousand, yes, about 25,000.

Q And with 25,000 members, where did that rate it in terms of size of the forum?

A It was a very large forum. You have more exclusive forums that are smaller membership, but that was probably one of the largest forums out there.

Q Was it a global forum, or was it focused on any particular geographic region?

A It was global.

Q And did the conversations on the forum all happen in English, or did they happen in different languages?

A No. So take it back a little bit in history -- I apologize. But so the carding forums, it's kind of a right to be on these forums. It's exclusive membership. So they all started off speaking English, because everyone -- it's kind of, like, the international -- everyone can speak English at some point. And so they would all start out in English.

Well, come to find out that when you spoke in English, the

law enforcement could actually read in English too, because it's believed that everyone in law enforcement can read English. So what happened was, at some point, they devised a plan, "Hey, let's create a Russian-speaking side," not necessarily just Russians, but anyone that could speak Russian could go on this side. And that way, we could speak in this language, and then you'll have another membership speaking a different language. Kind of -- I don't want to say hide, but maybe more exclusive on this forum, to be only Russian-speaking only. So there was two different aspects to the forum.

Q And once there became a Russian-speaking side of the forum, is there a reason why a carder who spoke Russian might still want to participate on the English side?

A Definitely. I mean, you still -- it doesn't matter if you speak Russian or English. You still get money. So they definitely wanted money from anybody. So they'll post on both sides.

Q Of the 25,000 members on carder.su, how many were endorsed by the site to sell credit card numbers?

A Just one, that I saw.

Q And did you become familiar with the nickname?

A Yes, sir.

Q And what was it?

A Track2.

Q Did you monitor track2's posts on the forum?

A I did, yes, sir.
Q And can you tell us what the general subject matter of those posts was?
A Just, like, he would go out there and claim he has all these credit card numbers, and that he's selling. And sometimes he'd give a price list and redirect you to a site that he would want you to go to to purchase his numbers. Just like any other small business, he would try to get as many people as he can and create this large advertisement to make sure people went to him first, because, you know, he wanted as much -- I guess as much sales as he could get.
Q What is a "profile page" on carder.su?
A So a profile page is -- you're going to log in. Any website, you create your own profile. You would have a username set up, whatever you want to be called, and then set up an e-mail so you can be communicated with, back and forth, and then any other information you'd want to give up. Normally, on something like this -- not normally, almost all the time -- you're not going to use your real identity. You definitely want to have an authentic e-mail, because that's the way that that forum will contact you, in case there's some kind of error, or someone does something, or they want to alert you of something. So you want to have that e-mail directly linked so you're able to grant access to it.
Q And was information like that displayed on the profile

page?
A It was, yes, sir.
Q Did track2 have a profile page on carder.su?
A Track2 did have a profile page.
Q Did you view that profile page?
A I did, yes, sir.
Q And I've placed Exhibit 8.8 on the overhead in front of you.
Is that a snapshot that you took of the track2 page?
A Yes, sir.
MR. WILKINSON: The government offers 8.8.
MS. SCANLAN: No objection.
THE COURT: 8.8 is admitted.
(Exhibit 8.8 was admitted)
BY MR. WILKINSON
Q It's a little small, so we'll blow it up.
Let's start with the top. What are we looking at, at the very top of the page?
A So if you look on the top, that's a banner. A lot of websites have them, just kind of an advertisement banner, of, you know, this is what's going on on the website. So if you look on the top left, the online dump shop, that's track2.name. That would be where track2 would want to redirect you to in order to purchase his credit cards. That, right there, is on all the time. It's on the top. Just if you visit the website,

there's always some kind of advertisement.
Q Okay. I'll just ask you a follow-up question to clarify.
So with that track2 name banner, was that banner there only because you were on track2's profile page, or is it a banner that would show up wherever you navigated on the carder.su website?
A That is -- wherever you navigated on the carder.su website, that would be on the top.
Q Okay. We've scrolled down a little bit, and we see the name "track2."
What's that?
A That would be the username you create on your profile page.
Q What does it say below that?
A Under that it's, "Trusted vendor of dumps," which that would -- because it's in green, green signifies its approval. Or like it says there, it's a trusted vendor, meaning the administrator, who I spoke earlier kind of controls the entire website, would give him an approval to sell, and that he is good-to-go. There's no kind of, like, fraud when you're purchasing stuff from him. Like, he's going to provide you good information.
Q And of the 25,000 members on carder.su, how many were listed as trusted vendors of dumps?
A Just track2.

Q Now we're down in the middle of the page.

Can you tell us what the purpose of this section of the profile page is?

A Sure. There's a couple different things. So this is kind of, like, a messaging thing, as if you all had Facebook. You would kind of create and see a picture, see a message, "Hey, this is a great picture." Well, this just verifies, "Hey, I need" -- there's a couple things -- "I need credit cards. Can you give me credit cards? I need numbers," you know, anything like that. Or it could also say, "Hey, track2 is great. He's done an awesome job by me," you know, just kind of make sure that you validate everything on that page. So that would be up there. And any time you went to the profile page, they would see, "Hey, this guy's good." "This guy's bad," or, "Hey, he's actually dealing with cards." You know, as you can see on here, it just requests he needs his services, he needs certain credit cards.

Q Okay. So we've scrolled down the page a little bit more.

What do you see in the upper left-hand corner?

A So if you look in the top, it just tells you when he joined -- when track2 joined the website, which is September 26 of 2009.

Q And then there's an item in the middle of the screen that says "reputation."

What's the purpose of that item there?

A To give a brief description of a reputation. When you're online, there is no face-to-face contact. There is only your reputation. So in order to have any kind of validity on a website, or on any of these forums, you need to make sure that your reputation is gold, your name is gold. Because once you get marked, you know, negative anywhere, no one is going to want to deal with you, especially that nickname.

So on this website it says his reputation is a ten, which is very high, so people know that, hey, track2 is good, his reputation is high, people have validated that he does what he says he does, and there's no question about what he's going to be doing.

Q You mentioned that you also viewed track2's posts.

Is Exhibit 8.9 one of the posts that you viewed, of track2?

A Yes, sir.

Q And does it accurately reflect that post? In other words, is it an accurate image?

A Yeah. Yes, sir. That is an image on a post that he would put on carder.su.

MR. WILKINSON: Government offers 8.9.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: 8.9 is admitted.

(Exhibit 8.9 was admitted)

BY MR. WILKINSON

Q Okay. Let's start up in the very upper left-hand corner of the screen.

What is the date of -- that this screenshot was taken?

A So that date is September 25, 2009.

Q And what is the join date, again?

A September 25, 2009.

Q So is this the date that track2 joined the forum?

A Yes. Yes, sir.

Q And what does the message here indicate, at the top paragraph?

A So it's indicating that there are dumps, or credit card numbers, for sale, and that he is -- that track2 is the one that grabbed those credit cards. It's not a resale. So he's the one that stole the credit cards, and now he's selling them. And he wants to forward you to his site, at track2.name, to go ahead and purchase these credit cards, these stolen credit cards.

Q Was there anything unusual to you about this posting being made on the same date that track2 joined the forum?

A Yes. It's kind of unheard of. So he already has reputation of ten, which is pretty high, significant. This is his very first day joining. And he has all of his credit card information for sale. On the same day he joins, he posts it, and he has a reputation. That doesn't happen when you're a

newcomer to a website, or a carding forum. You need to have some kind of validity that you are good. And as soon as he joins, his reputation has skyrocketed, and he already has his website going, and it's already there posted on a full-page shot on the website.

Q Is Exhibit 8.12 another posting by track2?

A Yes, sir.

Q And is that an accurate image of it there?

A Yes, sir.

MR. WILKINSON: The government offers 8.12.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 8.12 was admitted)

BY MR. WILKINSON

Q When was this posting made?

A That was June 7 of 2010.

Q And what is the posting here?

A He's posting to say he has 109,000 dumps, or he just stole 109,000 credit card numbers.

Q And does this mean that that's the total amount that he has for sale?

A No. That's just -- as you see, he just updated his website with 109 [sic] additional numbers.

Q You mentioned that you found it unusual that he sort of appeared out of nowhere, I think you said.

A Yes, sir.

Q Did you develop a theory as to how that could have happened?

A Yes, sir. So there was another vendor, quite similar in his language, and kind of did the same thing; went by the nickname nCuX. And he, at one point, said, "Hey, I'm retiring. I'm getting rid of all my credit card numbers. We're no longer going to be doing this. We're closing shop." You know, get it while you can.

So that ended, and within two months, all of a sudden, track2 appeared out of nowhere, and with all these credit card numbers available. As I said, he went on a website that had -- or a carding forum that had 25,000 members, stating that he can, you know, sustain any kind of requests at track2.name. If you have 25,000 members, and you join, and then you post that the same day, you have to have some kind of massive stolen credit card numbers database. I mean, you have to. It's just -- they wouldn't put him a number ten on that carder.su, as a reputation, if he couldn't back up what he was saying.

So my theory would be that nCuX retired, track2 took over -- well, nCuX grabbed the name "track2," created the online website, and just forwarded all those numbers that he had, and created a new website and a new nic, in order to sustain his business.

Q How long had the Secret Service been aware of nCuX

operating, before his retirement?

A A few years -- I mean, from my recollection, about 2007, from when I was -- from the databases we have.

Q Was nCuX also active on the carder.su forum?

A Yes, he was.

Q And is Exhibit 8.5 a posting by nCuX on that forum?

A Yes, it is.

MR. WILKINSON: Government offers 8.5.

THE COURT: Any objection?

MS. SCANLAN: Yes, Your Honor. The defense objects to Page 2 through 5 of this exhibit on the grounds that they are hearsay, and they are not established by the text as statements of co-conspirators.

MR. WILKINSON: Your Honor, I think I'd like to revise the offer and offer only Pages 1 and 2. So Page 1 is a party admission. Page 2 contains a carryover, which the top of it is still a party admission. The next two statements are statements about the defendant's reputation, and are admissible under Federal Rule of Evidence 803(21) as statements about a person's reputation within their community. They are also statements of co-conspirators, because they're people who have purchased from the defendant and were, therefore, part of the fraud.

THE COURT: Anything further, Counsel?

MS. SCANLAN: No, Your Honor.

THE COURT: All right. The Court will -- so you're offering just Pages 1 and 2, Counsel?

MR. WILKINSON: Yes, Your Honor.

THE COURT: And the objection goes to which pages, Counsel?

MS. SCANLAN: Your Honor, the objection was to Pages 2 through 5. So 3 through 5 are no longer offered. There was no objection to Page 1.

THE COURT: And just to be clear on the extent of the objection, it appears to the Court that the first two lines, on Page 2, look like a carryover or continuation of what's on Page 1. So I trust that the extent of your objection would go to just the -- basically the middle of the page, down, since there's no content in the middle?

MS. SCANLAN: Correct.

THE COURT: All right. The Court's going to sustain the objection from the middle of the page, down.

So Counsel, you need to redact Page 2. That's the Court's ruling. There's also highlighting on Page 2, Counsel.

MR. WILKINSON: There is, Your Honor. And that is embedded in the document -- actually, that's not in the original. That's just the display copy.

THE COURT: So the exhibit that goes back to the jury room will not be highlighted; correct?

MR. WILKINSON: That's correct, Your Honor.

THE COURT: Please proceed. The Court's made its ruling on the admission.

(Exhibit 8.5, Pages 1 and 2, was admitted)

BY MR. WILKINSON

Q Okay. So just to refresh, is this a posting by nCuX on the carder.su forum?

A Yes, sir.

Q Was this made before the appearance of track2 on that forum?

A Yes, sir.

Q And just looking -- let's look at the top left corner for a minute.

What are we seeing here, in the upper left corner?

A It's a pathway on the forum. So if you go on any other internet website, you kind of keep on clicking down. And it just shows you the path. Carder.su is the main, and then it goes all about security and network. English-speaking carders, as I said, it divided into two separate things, English speaking and Russian speaking. And then it goes into dump selling. And then from there, this dumps, referring to credit card information or credit card numbers that were stolen.

Q Okay. Now we're zeroing in on the middle of the page.

What do we see on the left side?

A That is a profile, the profile of nCuX.

Q Okay. And when had he joined?

A The join date was January 10, 2009.
Q And looking just up above there, can you see what date this screenshot was taken?
A January 10, 2009.
Q Okay. So is this the date that he joined?
A Yes, sir.
Q Okay. And what was his reputation there?
A As you see, he's rated as a newbie, or a new person on the website, so he had a zero reputation.
Q And we saw that track2 had a ten there before?
A Track2 had a ten prior, yes, sir.
Q So what would be the reason that this would be a zero?
A Just that he maybe just came on the website --
MS. SCANLAN: Objection. Calls for opinion testimony.
BY MR. WILKINSON
Q Based on your training and experience, what would be the reason that someone's reputation would be a zero on the day they appeared on the website?
MS. SCANLAN: I'm going to object to this witness testifying based on his training and experience. He's not endorsed as an expert.
THE COURT: Counsel?
MR. WILKINSON: I believe he was endorsed as an expert.

MS. SCANLAN: No.

MR. WILKINSON: Okay. I'll move on.

THE COURT: Objection sustained.

BY MR. WILKINSON

Q Okay. Can you tell us what the text of the statement says here? And you can read it or summarize it.

A Sure. It's basically telling individuals, whoever visit the website, his profile page, that he is a dumps provider. He does do everything himself. And he's looking for worldwide. He has worldwide access to credit cards. And then it gives a price list of all the credit cards. So if you're looking at in the U.S., you know, you have American Express, Visa, go different prices. Then you have -- credit cards, as you get a credit card, you're going to have a different level. You have your gold --

MS. SCANLAN: Objection. This is opinion testimony.

THE COURT: Let's clarify, Counsel.

BY MR. WILKINSON

Q Which credit cards are listed here?

A I was going to go through the gold, platinum, corporate, and the difference in the price limits that happen on credit cards. When you have a gold card, it's more than -- or less than a platinum --

MS. SCANLAN: Objection, I'm sorry. This is opinion testimony. He's not testifying about what he observed as a

fact witness on this exhibit.

THE COURT: That's sustained, Counsel.

MR. WILKINSON: Your Honor, I believe the witness has personal knowledge of this. He's not relying on other information outside of the scope of this, under Rule --

THE COURT: Let's clarify that through the examination, then.

BY MR. WILKINSON

Q Okay. Do you have personal knowledge of how these -- of how these different credit cards operate?

A Yes, sir.

Q And how have you developed that?

A Just through the website and purchasing, and then my own personal experience of credit cards.

Q Okay. And let's actually move up to the top of this page. It indicates, "Dumps from first hands, USA and EU."

Do you know what "Dumps from first hands, USA and EU" means?

A It means that he was the first one to grab them. They were not a resale.

Q Is that the same way that track2 --

MS. SCANLAN: Objection. Leading.

THE COURT: That's overruled, Counsel.

BY MR. WILKINSON

Q Is that the same way that track2 described the source of

his credit card numbers?
A Yes, sir.
Q Is Exhibit 8.7 another forum post by nCuX?
A Yes, sir.
Q And is it an accurate capture of that forum post?
A Can you repeat that, please?
Q Yeah. Is it an accurate capture of it?
A Yes, sir.
MR. WILKINSON: The government offers 8.7.
MS. SCANLAN: May I inquire?
THE COURT: You may.
VOIR DIRE EXAMINATION
BY MS. SCANLAN
Q Agent, did you create this screen capture yourself?
A No, ma'am.
Q Who created it?
A Part of our unit in the CIS lab that we have.
Q Okay. So you don't know if this is an accurate screen capture, right, because you weren't looking -- you're not the one who created it?
A I was not the one who created it, ma'am.
MS. SCANLAN: I object. This witness doesn't have the proper foundation for this exhibit.
MR. WILKINSON: May I continue to ask further questions?

THE COURT: You may. I'll reserve ruling on the objection, Counsel, depending on the balance of the foundation that counsel establishes.

DIRECT EXAMINATION

BY MR. WILKINSON

Q Does the CIS unit maintain a collection of screenshots like this?

A Yes, we do. Through all of the search warrants from servers, electronic media we've had throughout the years, we have a database of information that we go back and try to compare and contrast everything that goes on. And screenshots are part of that database we have, yes.

Q And were those -- that database, and specifically screenshots like this, something that you came to rely upon in your day-to-day work?

A Yes, sir.

Q And did you, in the course of your experience, find those screenshots to be a reliable source of information in your investigations?

A Yes, sir.

Q And did you become familiar with the way that they were stored in the CIS records?

A Yes, sir.

MR. WILKINSON: The government offers 8.7.

MS. SCANLAN: Your Honor, the defense has the same

objection. This is not a business record kept in a database that he has verified. It's a screenshot, and the witness doesn't know if it's an accurate screenshot or not, because he's not the one who created it.

MR. WILKINSON: Your Honor, that's a matter that simply goes to chain of custody, which would go to the weight and could be explored on cross examination. This has been established as a business record, and I think he's properly authenticated it.

THE COURT: Counsel, there's actually one additional question for a business record, that hasn't been asked, and the Court will sustain the objection until that's clarified, in order for this to be admitted as a business record.

BY MR. WILKINSON

Q Were these images generally captured at the same time -- was it CIS's practice to capture these screenshots at the time that they existed on the internet?

A Yes, sir, because you just never knew how long they'd be up there, so you capture them as soon as you can.

MR. WILKINSON: The government offers 8.7.

THE COURT: Objection is overruled now, Counsel. It's admitted.

(Exhibit 8.7 was admitted)

BY MR. WILKINSON

Q So to refresh, is this another posting by nCuX?

A Yes, sir.
Q And date on this posting?
A June 21 of 2009.
Q And what is he indicating here?
A That he sells dumps, and you can search all his website for particular BINs. He has a minimum order of a thousand dollars, and it offers different type of payment options. Through e-currency, we have either WebMoney, Western Union, or MoneyGram, are three different options. Then it just kind of gives you a price for, you know, what you're looking at, a breakdown, for USA, American Express, Visa, MasterCard, and Discover. Then below that, it goes to other countries, as well.
Q Does he make any particular announcement on this page about the future of his business?
A Yes. On July 20, he is going to be closing shop. As I stated earlier, he's going to retire, be done. He wants to get rid of all his numbers, so he's having this big liquidation sale of all these credit cards.
Q And following this announcement, did he, in fact, stop doing business on the internet?
A As far as we could see, yes, he was no longer anywhere we could find.
Q Okay. I'm pulling up Exhibit 8.9 on the right, can you remind us what that was?

A Sure. That was a track2 profile page -- or I'm sorry -- track2's, kind of, like, a selling page, that we talked about, where he redirected you to track2.name. And then it had -- on the left-hand side, it goes to show the -- you know, his join date was September 25 of 2009.

Q Okay. And how did that join date of September 2009 compare to the closing date of nCuX?

A It was approximately two months after the closing date.

Q At some point, did you make contact with track2?

A I did, yes.

Q And how did you reach out to him?

A ICQ, which is a messaging service that was hosted by AOL. Basically, it was text messaging through the internet, through the online application. And he would provide his number on carder.su, and you'd just text him and say, "Hey" -- whatever communication I wanted.

Like, I asked him if he had any numbers, if I could get on his website. He had told me, "No, the registration is full," which I took, maybe, you know, he couldn't support any more personnel. Then he redirected me to a second site that he had, called bulba.cc. Now, he said bulba.cc was his secondary site. And I had asked him, you know, "Are the numbers the same?" Because I heard, you know, his numbers are really good. They're fresh, meaning, you know, they were stolen within the past 30 days. So, you know, were they the same numbers? And

he confirmed that bulba.cc and track2.name were the same numbers, in fact.

Q Is Exhibit 16.15, which is -- 16.15, which is on your screen in front of you, a screen capture of that chat that you had with track2?

A Yes, sir.

MR. WILKINSON: The government offers 16.15.

MS. SCANLAN: Your Honor, I apologize. If I can just look at this one really quickly?

THE COURT: You may.

MS. SCANLAN: No objection.

THE COURT: 16.15 is admitted.

(Exhibit 16.15 was admitted)

BY MR. WILKINSON

Q How many people are parties to this chat?

A There's two.

Q And who are they?

A Myself, which is mmfujitsu, and track2.name.

Q What did you say to introduce yourself?

A I said, "Hey, how are you doing? I've talked to you before," to kind of get the feeling that we've worked in the past before, so he knew that, you know, maybe I talked to him. Whether I was on his address book, I don't know, but to kind of -- just to let him know we talked before.

Q And then what did you tell him after he had said, "Hello"?

A I told him I was on track2.name, but I was unable to log in or register as a new user.
Q Did you ask him a question?
A Yeah. I asked him if the -- I went onto bulba.cc, and are the numbers the same? And he had said, "Yes, they're the same numbers."
Q So after that, did you, in fact, go to the bulba.cc website?
A I did, yes.
Q Was it something you were able to enter immediately, or did you have to register?
A I had to register and provide information to it. Just like logging on to any other website, I had to provide a username and password, and then I got directed to the main site, after they confirmed all my registration information.
Q Showing you what's been previously admitted as Exhibit 2.1, is that what you saw when you landed on the bulba website?
A Yes, sir.
Q And were you able to successfully register?
A I was, yes, sir.
Q Did you have to pay money to register?
A No, I did not.
THE COURT: Counsel, why don't we let the jury take a stretch break.

Please be seated. You may continue, Counsel.

BY MR. WILKINSON

Q When you went onto the website, did you take screen captures of it?

A I did. I took screen captures and recorded a video of me on the website.

Q How did you record the video?

A Through a program called "Snagit." It would capture whatever I was doing on the computer.

Q Describe what you were doing when you captured the video?

A I was just surfing the internet, just to kind of detail what access you could have while you were on that, on that site. I would go on the dumps part, and it would give me the main screen here. And as you see, the main screen --

Q And let me stop you right there, because the jury can't see it on the screen yet. So if you'd describe --

A Okay. I apologize. So on this website, it would be comparable to, like, an Amazon website, where you can point and click, and purchase whatever you want. But this site was exclusive to stolen credit card information. You could pick American Express, Visa, MasterCard, whichever credit card you want. You could go by whichever country you want. If you had a specific bank you're looking for, there's, like, a search engine you could try to find any specific card you want. If you were living in Seattle, as you are, but you're traveling to

D.C., you most likely want a D.C. number, because sometimes when you're --

MS. SCANLAN: Objection. This is opinion testimony.

THE COURT: It's starting to go a little bit far afield, Counsel. Sustained.

BY MR. WILKINSON

Q I think we got a general sense of what you did there.

Is Exhibit 2.6 an accurate copy of the video that you captured?

A Yes, sir.

MR. WILKINSON: The government offers 2.6.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 2.6 was admitted)

BY MR. WILKINSON

Q So I'll start playing the video in a second.

But could you first just sort of orient us to where we are and what we're seeing?

A Certainly. This is the main page of the website bulba.cc. If you look on the left, I was talking about the drop-down menus, there's arrows there, that's where you can pick your banks, your region, your BIN numbers, which is the bank identification number, which coincides with the region that, A, you would live in, or that you want the credit card in. And then you could vary between any kind of credit card.

And then kind of going to the right, you have a checker, which would be, if you were to purchase all these credit cards, you can pay a small fee. If you pay the small fee, all these credit cards will be checked, for, like, a dollar or so, just to verify that they haven't been alerted as stolen. So if it went through, and you paid the checker, you know, "Hey, I got 'X' amount of days in order to use this credit card, because right now it's good-to-go to be re-encoded, or used."

And then if you continue to the top right, there's a basket, in-box. That's kind of what you purchase in your checkout. Below that is a quick buy. So if there are older cards, you can purchase a certain amount for less money. The bulba.cc -- or he would not verify that they're good or bad, but you purchase, like, a thousand or 10,000 cards for a little bit of money in hopes that all of these weren't claimed as fraud yet. So he would still be making money off his older credit cards.

And then below, the major part of this entire website is just the list of credit cards that are available. So you have -- right there, it talks about American Express, and then the codes. And then if you go further apart, it says how many he has. So on the third line, he has 14 or 18 American -- I can't read the number. I apologize -- but how many American Express cards he has, and then how much they are, and then how many do you want to purchase.

So if you're going there, you see -- that's on Page 1. He has 398 pages of all these credit cards. So if he -- if he is the provider of credit cards on carder.su --

MS. SCANLAN: Objection, narrative. And it's beyond the scope of the question.

THE COURT: I'll sustain on the narrative component, Counsel.

BY MR. WILKINSON

Q What did this -- the fact that there were 398 pages of lists of stolen credit cards tell you about what you'd found on carder.su?

MS. SCANLAN: Objection. This calls for opinion testimony.

THE COURT: That's overruled.

THE WITNESS: He has hundreds of thousands of stolen credit cards that are accessible through this website.

BY MR. WILKINSON

Q Was that consistent with him being the only vendor of credit cards on carder.su?

A Yes, sir.

Q Okay. So I'm going to push "play" now. And please feel free to narrate, as the video goes along.

(Video recording was played)

A Again, this is just me navigating through. So I was looking at United States of America credit cards. And then I

have a whole list of banks that are available in the United States. And just -- as you can see, there's just hundreds of them that are on there.

(Video recording continues)

A And then as I said, they're all different types of credit cards, either Visa, American Express, Discover, whichever he has available.

Now, when I'm searching this, I'm just randomly picking. I wasn't specifically looking for something. So when I do hit "search," it doesn't come up with any hits, because I just randomly picked banks. But if I were to look at that bank, you know, if I had a specific one I was looking for, and it had those located on that website, it would come up with how many credit cards from that specific search I did.

Q Is this searching right now?

A So the search, as you see, nothing came up. Just randomly picked a bank.

Q It looks like the bank that you picked, Banco Popular North America?

A Yes, sir.

Q Was there any reason you picked that?

A No, no reason at all.

And this here describes the checker, as I was saying, the small fee, you can check all the credit cards you purchased to see if they were still active, in order to be used. So it just

lists -- like, if you do a hundred, it's $50, 500, $50 [sic], so on and so forth.

Now, this here was a program issue. So Snagit probably didn't have enough memory in order to keep on going, so that's why it was flickering. That wasn't the website itself.

And then I just clicked on "all," just to have a whole gamut of lists. And on here, you could also export your credit cards you purchased to a text file that will list all the credit cards that you have purchased.

BY MR. WILKINSON

Q Did you investigate the registration information for the bulba website?

A Yes, I did. I used DomainTools in order to investigate that.

Q And what is DomainTools?

A That is a basic search engine for a website. So if you have -- whatever website you want, it will give you the registration information for that particular site, or that IP address.

Q Showing you Exhibit 4.4, which has been previously admitted, is that the DomainTools report for the bulba website?

A Yes, sir.

Q Did you look to see what the e-mail account used to register the bulba website was?

A Yes, I did.

Q And what was that e-mail account?
A It was bulba.cc@yahoo.com.
Q Is that it right there?
A Yes, sir.
Q And looking at Exhibit 17.7, which has been admitted for demonstrative purposes, could you just use your finger and point out where on this diagram the bulba.cc website is?
A It's in the top right corner.
Q Right there (indicating)?
A Yes, sir.
Q Did you get a search warrant for the contents of that e-mail account?
A Yes, sir, I did.
Q And by the way, who were you working with when you were executing the search warrants? Were you working with anyone local, in Seattle?
A Yes, sir. I worked with Detective Dave Dunn, who was on the Secret Service task force, with the Seattle Police Department.
Q And he testified earlier about some of these other warrants that were executed, rubensamvelich and the booookscafe.
Did you also participate in those warrants?
A Yes, I did.
Q So were you able to successfully get a warrant for this bulba.cc website?

A Yes, sir, I was.
Q And in terms of volume of contents, how did the volume of this one compare to the other two?
A It was the least amount of volume, or the least amount of e-mails on the return.
Q Do you recognize Exhibit 7.1?
A Yes. That is the bulbacc Yahoo! account.
Q And is this part of the information that came back from this return?
A Yes, sir, it is.
Q Is this subscriber information about who took out the account?
A Yes, sir.

MR. WILKINSON: Government offers 7.1.

MS. SCANLAN: No objection.

THE COURT: 7.1 is admitted.

(Exhibit 7.1 was admitted)

BY MR. WILKINSON
Q So what do we have up here, in the first line?
A That would be your Yahoo! username.
Q And then can you tell us what the registration IP address is?
A So wherever you registered that account from was the IP address that was used for that registration.
Q So -- and what do you mean "registered it from"? Is that

the computer --
A The computer he registered it from would be the -- it returns to that IP address.
Q And so putting that next to 17.7, was this server related to -- or connected to this IP address, rather?
A Yes, sir --
Q Was it related to any other server that you saw elsewhere in the investigation?
A Yes, sir. That was related to the HopOne server, located in Virginia.
Q So this one down here?
A Yes, sir.
Q Now, the IP number looks a little different.
Can you explain why that is?
A Because he had three different IP addresses located at HopOne. And one of them was the IP address ending in .124.
Q Was this .124 one co-located with the one that's on the diagram?
A Yes, sir.
Q Pulling up Exhibit 7.2, is that IP logon information for the bulbacc e-mail account?
A Yes, sir. That would be the times he logged in using bulba.cc. And it recorded the IP address and the dates and times he would log in.
Q Was this information that came back in response to the

search warrant?
A Yes, sir.
MR. WILKINSON: Government offers 7.2.
MS. SCANLAN: No objection.
THE COURT: Admitted.
(Exhibit 7.2 was admitted)
BY MR. WILKINSON
Q Is this -- so we've got a list of IP addresses here.
What is this list intended to capture?
A It intends to capture which IP you're logging in from, or the location that you're logging in from, and then the date and the time of that login.
Q So we have a date range here. Can you tell us what that range is?
A Sure. September 23, 2009, through September 21 of 2010.
Q Okay. So about a year?
A Approximately a year, yes, sir.
Q And how many times did the user of the bulbacc account log on over that year?
A Four times, sir.
Q And which server did they use all four times?
A The one ending in .124.
Q Did you participate in the search and seizure of the HopOne server?
A Yes, I did.

Q And did you identify information on there linking the server back to any particular individual?
A Yes, sir. We located all the information coming back to a Roman Seleznev.
Q Is Exhibit 7.3 a series of e-mails that came back with the search warrant from the bulbacc account?
A Yes, sir.
Q And are they all from WebNames.ru?
A Yes, sir.
Q And is WebNames -- what is WebNames.ru?
A WebNames.ru is kind of, like, a GoDaddy, where it has a group of IP addresses that you can purchase. And that's what this e-mail is reflecting, is that he registered the website "bulbacc" with WebNames@ru [sic]. And this is showing a login and a password for that.
Q And then it's a multipage document. Are there other e-mails from WebNames.ru?
A Correct. So if you're going to purchase something, they send you an invoice. And he received an invoice for the amount of approximately $33 for a year-long subscription, registration for bulba.cc. And continuing, we found that it -- he did pay the $33 through a -- I believe it was a WebMoney account that he would forward the money for the registration for the year.
Q Are these e-mails that are automatically generated by WebNames.ru?

A Yes. And once you register, it's going to bill you, either the administration or automatically generated as you register.

MR. WILKINSON: Government offers 7.3.

MS. SCANLAN: Your Honor, I object that this witness doesn't have the proper foundation to testify that these are machine-generated e-mails.

MR. WILKINSON: Your Honor, a previous witness has already testified that web hosting -- or web registration companies, by practice, automatically generate e-mails of this nature.

THE COURT: The objection, on those grounds, is overruled. 7.3 is admitted.

(Exhibit 7.3 was admitted)

BY MR. WILKINSON

Q Looking at the first page of 7.3, what is the date of the e-mail?

A Date is April 26 of 2010.

Q Okay. And who's it from?

A It's from WebNames.ru support, or the -- that is an automatic generated web address.

Q Okay. And remind us, because this was before we had the exhibit, what is WebNames.ru?

A It's a hosting site that contains a bunch of IP addresses that you can purchase.

Q And what site were they writing about in this e-mail?
A They were -- they wanted to -- this e-mail was in reflection to bulba.cc.
Q And what was the subject?
A The registration, his registration.
Q And if we look down, it looks like we've got Russian on the top half, and it's translated into English at the bottom?
A Yes, sir.
Q What do we see at the bottom half, in English?
A It's just, you know, basically your welcoming e-mail; that you logged in, and you have provided a username and a password. And it's just a reiterating what you provided in the website.
Q And what is the specific logon?
A The login is "bulbacc," with a password "telkom135."
Q And we are going to skip to 7.3A, which is the English translation of the same document. And let's go to the second page of the exhibit now.

Another e-mail from WebNames?

A Yes. Another e-mail from WebNames. As I was saying before, you get an invoice, once you purchase something, and that is exactly what this is. They're invoicing him for the $33.82 U.S. dollars in order to access an IP from that provider.

MS. SCANLAN: Your Honor, I'm not sure this is an admitted exhibit.

MR. WILKINSON: This is -- this is the translation.

MS. SCANLAN: I know what it is, but I don't think you offered 7.3A.

THE COURT: 7.3A was previously admitted, Counsel, on 8/16.

MS. SCANLAN: I apologize.

MR. WILKINSON: Because all of the translations came in.

BY MR. WILKINSON

Q Okay. So this is an invoice for $33?

A Yes, sir.

Q And then we have another e-mail. What's the date on that?

A That's April 26, 2010.

Q And what's this saying?

A That his payment for the invoice that they sent out was paid.

Q Okay. So the $33 was paid?

A That's correct, sir, yes.

Q And then we have another e-mail, on the sixth page of the document.

What does this one indicate?

A That it's going to be registered for a year from the date of registration. And it will be on DomainTools in a couple days, after the registration is complete internally.

Q Were there e-mails in this account specifically tying the

account back to any particular user identity?
A No. This one was just registered just back to bulba.cc. Or -- sorry. I should say, bulbacc@yahoo.
Q I want to go back, just for a minute, to nCuX. We talked about him a little bit.
Did nCuX register websites?
A No. I mean, did he register his own website? Yes, he did. I apologize.
Q And did you conduct research into the registration for those websites?
A Yes, I did.
Q What is Exhibit 4.3?
A That is a DomainTools report for nCuX.tv.
Q And is that one of the websites that you researched?
A Yes, sir.
MR. WILKINSON: The government offers 4.3.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 4.3 was admitted)
BY MR. WILKINSON
Q So is this just the cover page of the report?
A Yes, sir. It's the front page.
Q And we're going now to the seventh page.
Is this the registration information for nCuX.tv in 2009?
A Yes, sir.

Q And what was the name it was registered in?
A Andrey, and the last -- I don't know how to pronounce that. It's V-M-O-T-L-A.
Q And was there an e-mail?
A There was. Booookscafe@yahoo.com was the e-mail provided.
Q Did you conduct similar research for two other nCuX websites?
A Yes; the nCuX.name and .asia, A-S-I-A.
Q And is Exhibit 4.14 a summary of the registration information for those sites?
A Yes, it is.
MR. WILKINSON: The government offers 4.14.
THE COURT: Any objection?
MS. SCANLAN: Yes, Your Honor. The defense renews the objection that this is not a necessary summary exhibit, because the underlying reports are not voluminous or hard to understand.
THE COURT: Objection is noted. Overruled. It's admitted.
(Exhibit 4.14 was admitted)
BY MR. WILKINSON
Q So what do we have in the left column of this?
A That's the domain name that was registered.
Q Do those all begin with "nCuX"?
A They're all nCuX.name, .asia, .tv.

Q And how do the creation dates compare?
A They're all the same dates.
Q And the name?
A Same name, phone number, and registered address, as well as the e-mail.
Q And what is that e-mail account?
A It's boookscafe@yahoo.com.
Q And did you participate in the search of that boookscafe e-mail account?
A Yes, I did.
Q And did you find items in that search linking that account back to any individual?
A Yes, sir. We located the name "Roman Seleznev" in the boookscafe e-mail account.
Q Did you find photographs in there?
A Found photographs from Vkontakte. It's like the Russian Facebook, as well as a flowers website where he purchased flowers.

MR. WILKINSON: No further questions, Your Honor.

THE COURT: Members of the jury, if you just want to stand quickly before we begin cross examination?

Cross examination?

MS. SCANLAN: Thank you, Your Honor.

THE COURT: You may begin.

////

CROSS EXAMINATION

BY MS. SCANLAN

Q Agent Wojcieszek?

A Good morning, ma'am. Yes, ma'am; Wojcieszek.

Q Good morning.

Did you do research at some point into how many people named "Roman Seleznev" lived in Vladivostok, Russia?

A Yes, ma'am.

Q And do you know the approximate size of Vladivostok?

A I do not, no.

Q Maybe about 200,000 people?

A I would have to take your word for it. I do not know, ma'am.

Q How many "Roman Seleznevs" did you find in Vladivostok?

A From my recollection, two, from my recollection; the father -- his father, and the son.

Q And then let me show you something; okay?

A Certainly, ma'am. Yes, ma'am.

MS. SCANLAN: May I approach?

THE COURT: You may.

THE CLERK: Defense Exhibit 111 is marked.

BY MS. SCANLAN

Q Okay. Agent, I just want you to read that, not out loud, but to yourself; okay?

A Yes, ma'am.

Yes, ma'am?
Q So there was a total of three "Roman Seleznevs" that you identified as being in Vladivostok; correct?
A That's not what I gather from here, ma'am. What -- I have two individuals that I found. And then as we went on the websites, the social networking website, Vkontakte, we found Roman Seleznev with a different date of birth and different photographs. I don't think that I thought it was three. I just thought it was two different, at the time.
Q So we have two "Roman Seleznevs" that you identified, that have addresses in Vladivostok; correct?
A That was through, like, a phone book. Now, a phone book is a little bit different -- yes, ma'am.
Q Listen to --
A Yes, ma'am.
Q -- my question --
A Yes, ma'am.
Q -- all right?
Okay. So there's two. And then there's a third Roman Seleznev that you identified having a date of birth in 1990, who lists his hometown as Vladivostok on a social networking site; correct?
A Yes, ma'am.
Q So that's a total of three; correct?
A Those are three different ones you said right now, yes,

ma'am.

Q Okay. And two of those, actually, it's not just "Roman Seleznev," it's "Roman" -- now, this is going to be bad, the middle name -- "Valeryevich."

Do you know what I'm saying?

A Yes, ma'am.

Q "Seleznev." So there are two people with the same first name, middle name, and last name, who live in Vladivostok, Russia, according to the phone directory you looked at.

A Yes, ma'am.

MS. SCANLAN: I have nothing further.

THE COURT: Redirect, Counsel?

REDIRECT EXAMINATION

BY MR. WILKINSON

Q So we're looking at Exhibit -- Defense Exhibit 111, that was just shown to you.

What is the address listed on there?

A It is -- the number is 436530 Prospekt -- I can't pronounce that. I apologize -- O-S-T-R-Y-A-K-O-V-A, House Number 26, Apartment 113.

Q Did you do a web search to develop that address?

A Yes, sir.

Q Was that on a website called SpravkaRU?

A Yes, sir.

Q I'm showing you Exhibit 16.7.

Do you recognize that?
A Yes, sir.
Q And is that the web search that you did?
A Yes, sir.
MR. WILKINSON: The government offers 16.7.
THE COURT: Any objection?
MS. SCANLAN: Your Honor, if I may have one moment?
THE COURT: You may.
MS. SCANLAN: May I inquire?
THE COURT: You may.
VOIR DIRE EXAMINATION
BY MS. SCANLAN
Q Agent, this SpravkaRU.net, do you know what that is?
A Yes. It's basically a phone book for the area, online.
MS. SCANLAN: I have no objection.
THE COURT: 16.7 is admitted.
(Exhibit 16.7 was admitted)
REDIRECT EXAMINATION
BY MR. WILKINSON
Q So we've got it next to Exhibit 12.6B, which has already been admitted.
So on the left, are we looking at the source of the address that you looked up online?
A Yes, ma'am -- or, sir. I'm very sorry.
Q And 6.7A has been admitted as the translation of that

document.

And can you read the address there?

A It's 26 O-S-T-R-Y-A-K-O-V-A, Prospekt, Apartment 113.

Q And now we've got the defendant's passport on the right.

Can you read that address?

A It's the same address as I just read, yes, sir.

Q I also want to show you Exhibit 3.16A. It's been previously admitted.

Is that one of the images that was found on the HopOne server?

A Yes, sir.

Q And remind us what the HopOne server was.

Was that one of the servers used for part of the criminal infrastructure?

A Correct. That was the server that used the three IP addresses for all the e-mail accounts.

Q And now I want to show you Exhibit 12.7, on the left -- 12.7A, rather.

So what is the passport number on this passport?

A It's 6404 -- sorry. I think it's -- I0831 [sic].

Q And the passport number found on the HopOne server?

A Identical, 640410831.

Q In your experience, do passport numbers tend to be unique?

A Yes, sir.

MR. WILKINSON: No further questions.

THE COURT: Anything further, Counsel?

MS. SCANLAN: No, nothing further.

THE COURT: Any objection to this witness being excused, by the government?

MR. WILKINSON: No, Your Honor.

THE COURT: By the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you, sir. You may step down and be excused.

We'll take our morning recess at this time.

THE WITNESS: Thank you, sir.

(Jury exits the courtroom)

THE COURT: Counsel for the government, anything to take up?

MR. WILKINSON: No, Your Honor.

THE COURT: Counsel for the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: We'll take our recess.

(Recess)

THE COURT: Counsel, resume the testimony of the agent?

MR. WILKINSON: Thank you.

MICHAEL FISCHLIN, having been previously sworn, was examined and testified as follows:

DIRECT EXAMINATION

BY MR. WILKINSON

Q Welcome back, Inspector Fischlin.

A Thank you.

Q When we left off yesterday, we were looking at the image of the defendant's desktop.

Can you tell us, as an investigator, is it useful to you to know what kinds of items a subject stores on their desktop?

A Yes.

Q And why is that?

A Well, you can see the desktop as a user sees it, which is valuable. Another thing is, people usually put things they want quick access to on their desktop, so it gives you an idea of an individual's preferences.

Q So we were looking down at this lower left-hand corner of the screen -- or excuse me -- lower right-hand corner of the screen.

And can you refresh us on what this box that said "gift.jpg" was?

A Yes. It's a graphic image of gift cards. Seemed to be a generic image of Visa gift cards.

Q How are Visa gift cards used in the carding industry?

A They can be used to re-encode track data onto those cards, so that they can then be used at merchants, physical merchants.

Q And then the next image, over to the right?

A That is a graphic image of an MSR206, which is a magnetic stripe reader/writer.
Q And remind us how those items are used in the carding industry.
A That device is a piece of equipment which can be used to actually write credit card data onto the magnetic stripe found on the back of, say, a gift card or credit card. That's the hardware you'd use to facilitate that process.
Q And immediately below that, I see some text that says "banner.gif."
Is that the name of a file?
A It is.
Q And did you open that file?
A Yes.
Q And what is that file?
A It was an animated file. In particular, it was an ad for the domain 2Pac.cc.
Q Did you review Exhibit 13.6 before coming to court today?
A Yes.
Q And is that a capture of that animated ad that you saw?
A Yes. That's the ad, once opened.
Q Does it accurately depict what would happen if you clicked on that ad on the desktop?
A Yes.
MR. WILKINSON: Government offers 13.6.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.6 was admitted)

BY MR. WILKINSON

Q All right. So if I push "play," will we see what you would see, if you clicked on it on the desktop?

A Correct.

(Video recording was played)

BY MR. WILKINSON

Q Do you recognize the person in the image there?

A Yes.

Q And who is that?

A That's the rapper -- or was the rapper, Tupac.

Q What's the rapper Tupac's full name?

A Tupac Shakur.

Q Okay. So we're back to the desktop. Let's zoom in now on the upper left corner of the desktop.

What do we see -- without going into the name of it, but there's a little -- looks like a folder there. What kind of an icon is that, or what does that signify?

A It's an icon showing the logged-in user.

Q What does "logged-in user" mean?

A That would be the user account. Once -- after logging into the device, that would be the user account that you're actively in.

Q And on a Windows computer, who sets the name of the user account on the computer?
A Someone with access to the device, that would establish the account.
Q Would that include the owner of the computer?
A Absolutely.
Q And what is the username of this computer?
A When logged in, the user profile was "smaus."
Q Could you spell that?
A S-M-A-U-S.
Q And was that a word or name that you or Detective Dunn had seen earlier in the investigation?
A Yes. Detective Dunn had linked that nickname to the defendant.
Q Putting up Exhibit 17.7, and using your finger, which I think if you put it on the screen it will show up, could you circle the items on here that were -- that were linked to the word "smaus" in the investigation?
A Sure (indicating).
Q So we've got the HopOne server?
A Correct.
Q And how did it show up on the HopOne server?
A It appeared on the HopOne server within -- within, seems like, registration-type e-mails. It appeared as a username, in particular, at various times, on that server.

Q And then you just circled the "boookscafe" e-mail.
Did it also show up in that e-mail account?
A Yes, it did, in the same way, e-mail content showing that it had been used as a username for different accounts.
Q Anywhere else on this diagram where the "smaus" username was used?
A Yes (indicating).
Q You're marking the "shmak" or "smaus" server.
I guess it's obvious, but how did it show up there?
A It was a server that was found to host malware in the case.
Q And anywhere else on here where the smaus username was used?
A It may have, but not to my recollection at this time.
Q Let's just put that on a split screen. I'm calling up Exhibit 6.7, which was previously introduced as an e-mail from the rubensamvelich account.
Do you see that rubensamvelich account on the screen?
A I do.
Q Okay. Can you put a circle around that?
A (Indicating)
Q And is this an e-mail to the rubensamvelich account?
A It is.
Q Okay. Is it talking about registration on an investment site?

A Yes.
Q And what is the login and password on that?
A Login is "smaus1," and the password is "ochko123."
Q And remind us, that "ochko123," did you testify about using that yesterday, in your investigation?
A Yes. It was the same password as I found for the laptop.
Q The laptop that was seized from the defendant?
A Correct.
Q Okay. Back up to this upper left-hand corner of the defendant's desktop, any other items on here that you noticed?
A One on -- within this screenshot is a MultiBit, was of interest.
Q What is MultiBit?
A It is a desktop Bitcoin wallet, used to store and transact in Bitcoin, which is a digital currency. It's also a form of payment accepted on a domain that became of interest, 2Pac.cc.
Q So 2Pac accepted Bitcoin?
A Yes.
Q And what about down here in the lower -- towards the right-hand corner, "Tor" browser, what's that?
A That was software for Tor, which is software which can be used to browse the internet in an anonymous fashion. It also allows the user to access the deep web, which are areas of the internet which are inaccessible to traditional browsers, such as Internet Explorer, Firefox.

Q Let's move on to a different topic now.

Can you tell us what a "hosts file" is?

A Yes. It's a native file, found on Windows operating systems. It sort of acts as an address book. And it contains IP address to domain name mappings. And the best way I can explain is -- to just sort of give you an example of how it works, because the rest is kind of complicated.

So if you open up an internet browser, and you want to browse, let's say, "mysite.com," your computer is first going to check the hosts file on that computer to see if it knows the IP address for that site. If there's an entry in there for it, it will automatically go to that site. However, if there's not an entry for that site, now the computer is automatically going to reach out to a domain name server. And it does that to figure out, "Hey, what is the IP address for that site?" DNS server will give your computer that address, and then you can go to the site. So that is how that process works.

Q So what's the benefit of me setting up a hosts file on my computer?

A Well, it's on the native file, so it exists. But the benefit of modifying it, containing IP address domain name mappings is, one, you may notice faster navigation to the site, because your computer no longer has to reach out to a DNS server. It knows the IP address for that site. So that's a potential benefit.

Q As an investigator, is a host site something you're interested in looking on a subject's computer?
A It can be.
Q And why? What does it tell you?
A Well, it can give you an idea of sites that a user frequently, maybe, visits, or that they have interest in, if there's a particular mapping contained in the hosts file.
Q Did you open the hosts file on the defendant's laptop computer?
A Yes.
Q And had it been modified to add any IP addresses for any specific sites?
A Yes. There was one addition to it.
Q And did you verify what that IP address -- what site that IP address was associated with?
A Yes.
Q Which site was it?
A 2Pac.cc.
Q Calling up Exhibit 13.8, do you recognize it?
A I do. That's the hosts file from the laptop.
Q So this is an image of the file taken off the laptop?
A Yes. This is a screenshot of that file.
MR. WILKINSON: The government offers 13.8.
THE COURT: Any objection?
MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.8 was admitted)

BY MR. WILKINSON

Q Okay. So let's start at the top. Now, I notice it says this is a sample hosts file used by Microsoft.

Does that mean this isn't a real one?

A No. It's a real file.

Q Do you know what that language is, "This is a sample hosts file"?

A That's just standard language on every hosts file that's defaultly [sic] found on a Windows-based computer.

Q Okay. Can you direct me to which portion of the text here shows where the user went in and added an IP address?

A Yes. That's the very bottom line.

Q Right down here (indicating)?

A Correct.

Q And what is the number starting with "46"? Do you know what IP address that -- or what website that IP address is associated with?

A Yes. That IP address was for 2Pac.cc.

Q And was the language "2Pac.cc" sitting in the hosts file, as well?

A Yes. That would be for the correct mapping. So when the computer tries to go to 2Pac.cc, it already has the IP address, as you can see, so it can navigate to that site.

Q What information do you need about a website to configure your hosts file so that it will work?
A You need the domain name, which in this case is 2Pac.cc, and then you need the IP address.
Q Was the -- this IP address, 46.125.231.15 [sic], was that publicly available?
A It was not.
Q Why not?
A Because the site was utilizing a service from Cloudflare for DDoS protection. And as a result, if you publicly tried to look up information on the site, you'd see Cloudflare's IP address, and not the true IP address for 2Pac.cc, which was contained in this file.
Q So if you had done internet research to determine 2Pac's IP address, would you have come up with this address?
A No.
Q How would you -- if it's not publicly available, who would know the IP address, or how would that information be available?
A Someone with intimate information of the site, such as an owner.
Q Please tell the jury what a "RAR" file is.
A It's just like a zip file. It is a compressed file.
Q Did you find any RAR files of interest on the laptop?
A Yes. There's a variety of RAR files on the laptop, of

interest.
Q And calling up Exhibit 13.13, is that one of the RAR files that was on the laptop?
A That was the contents of one of the RAR files from the laptop.
Q Okay. And the jury can't see it yet, but can you just tell us, generally, what was contained in this RAR file that you found?
A There was this HTML file, as you can see, which appeared to be for a web page. There was also some graphic files within it, as well as a 2Pac ad, which we just saw on the desktop. Both images of the gift cards and the MSR206, that we saw on the desktop, were also found in this .RAR file.
Q Was there also text in the RAR file, writing?
A There was, which you can see on this file, which appeared to be a web page.
Q What was the general subject matter of that text?
A It appeared to be a tutorial on how to manufacture a counterfeit credit card.
Q And is Exhibit 13.13 an accurate capture of the contents of that RAR file?
A Yes. That's some of the content of that file.
MR. WILKINSON: Government offers 13.13.
MS. SCANLAN: No objection.
THE COURT: It's admitted.

(Exhibit 13.13 was admitted)

BY MR. WILKINSON

Q So it looks like we're looking at a variety of things, pictures, links, and text; is that right?

A Correct.

Q Let's start with the text at the top of the screen. Can you just read that for us, please?

A "This is tutorial how to buy dumps and use in store (POS) (Make and using fake credit card). Here I will explain you how to earn money from $500 to $50,000, even $500,000. Remember this is illegal way. Process from the start to the finish."

Q And then is there a link below it?

A There is. There's a hyperlink for 2Pac.cc.

Q A little copyright symbol next to it?

A Yes.

Q What do we see below that, where it says, "The best dumps market"? Is that something we've seen today already?

A Yes. That was the ad we saw earlier for 2Pac.cc.

Q And then there are four items here. What is this?

A Headings or categories for different portions of this page.

Q Like, a table of contents?

A Yes.

Q What is Item 1 in the table of contents?

A "Choosing and buying equipment."

Q Okay. And Item 2?
A "Choosing and buying dumps."
Q Item 3?
A "How to generate Track 1 and why they needed."
Q What is Track 1?
A Track 1 is the first track found on the magnetic stripe on a credit card. It contains a credit card number, and also contains a person's name on the card.
Q And what's the fourth topic area listed on here?
A "Writing dumps on plastic."
Q And then did you find that these headings corresponded to something else within the document?
A Yes, more of an explanation about those items.
Q So let's go to Item 1. And remind us what topic area "1" was?
A "Choosing and buying equipment."
Q Okay. And why don't you read that entry to us, please.
A "The main and only one device you need to buy MSR206. There are many method you can buy it. It fully legal device, and can you buy it on eBay." And then there's a link.
Q And do you know what that link goes to?
A Yes. It would be for an MSR206.
Q And there's an image below that.
Is that an image, that specific picture, something that you saw elsewhere on the computer?

A Yes. This is an image for an MSR206. And again, that same image was found on the desktop of the computer.
Q That was the little square that we looked at a few minutes ago?
A Correct.
Q Let's go to the second page of 13.13.
Is this a carryover of that first section?
A Yes.
Q Okay. And what is it providing at the top?
A Another link for an MSR206.
Q And then now we're on to Part B of this description.
What does Part B cover?
A Discussing the purchasing of prepaid cards, or gift cards.
Q What does it say?
A "You need to buy also prepaid cards or gift cards of any banks or any store. (They must be with magnetic stripe), also at eBay or any place." And then there's a link for prepaid gift cards.
Q And then there's an image here.
Is that an image that you saw elsewhere on the laptop?
A Yes. That image was also found on the desktop of the computer.
Q So now we are on to Item 2. Remind us what Item 2 was.
A This section is discussing choosing and buying dumps.
Q Okay. And please read to us what it says about choosing

and buying dumps.

A "First what is dumps? That's a information that you can write on magnetic stripe of credit card (gift card) to make a copy (clone) of real credit card of which is stolen from cardholder. Like we already have equipment to write on magnetic stripe and have gift cards. Now we need a dumps. You can buy dumps in internet shop called 2Pac.cc. That's only one real shop who is legit, and they have mostly all dumps from the world. More than one million of stolen dumps."

Q And what's the image right below there?

A That is another ad for 2Pac.cc. Again, we saw that same ad on the desktop of the computer.

Q Let's continue on with a lesson on choosing and buying dumps.

What do we see next?

A More information for -- on how to buy dumps, methods of payments accepted, more data for registering at 2Pac.cc.

Q Is this talking specifically about signing up at the 2Pac website?

A It is.

Q And read that first paragraph to us, please.

A "You must first register in that shop. Registration is free and available for anyone. Just click 'sign up' there. Enter your username and password and click 'I agree with terms of service,' click 'sign up.' Now you can log in to shop and

start buy dumps."

Q And then does this next paragraph explain the ways that you can pay?

A Yes.

Q What's this next line talk about?

A How you can choose the dumps that you want.

Q And why don't you go ahead and read the rest of this section.

A "How to choose dumps we need. Because support of shop is too busy to recommend dumps which is needed for use in our city, I can give some advice. Method Number 1, when you enter a shop, you can see 'dumps.' Click there. There you can see BIN (is first six digit of credit card number, which mean what bank is it and which type of card is it, like gold, platinum, plastic [sic]). Example, if we live in state, New Jersey, we have branch in our state, or even city, 1st Constitution Bank. Then we choose bank this bank in shop and click 'search.'"

Q And turning over to the next page, what is this telling us about?

A What the result would be of such a search on that site.

Q Okay. So what is this list here? What is the result that we see?

A It would be results for that bank, United States 1st Constitution Bank, how many, and then what the price would be.

Q What was the price for these dumps?
A Fourteen dollars.
Q Would that be per card?
A I don't know if it was per card or for the whole 14 that were listed there.
Q Okay. Does the page also describe another method for searching for dumps on 2Pac?
A Yes.
Q And what is this one?
A Method Number 2, it says, "Go to 'dumps.' There you can see state, search our state, and click 'search.' By that way we receive BINs and dumps, which is used in our state. We can by they also."
Q And what about Method Number 3?
A "Go to 'dumps.' Click 'mix pack (buy bulk).' There you can buy 100 pieces from cheap price random. You can use all 100 dumps. Some may work, some no. But this way, you can understand which BINs work in your area."
Q Moving on to the fifth page, I won't ask you to read this whole thing, but what is Part 3 talking about?
A How to generate Track 1 for a credit card and why that's needed, in particular. That would be needed for some transactions to be successful.
Q Does it describe a method in there for generating Track 1 from Track 2?

A Yes.
Q Let's look at Item 4. What does this cover?
A Writing dumps on plastic, or actually transferring the dumps to a gift card, for example.
Q And what does the first line say?
A "We need software to connect our MSR206 with computer and write on magnetic stripe of our gift card."
Q And then the next line?
A "Download it here, the JeRM."
Q And what does that underlining there mean?
A It's a hyperlink so you can download the program.
Q Okay. So is that a piece of computer software?
A Yes.
Q And did you find computer software called "the JeRM" on the defendant's computer?
A Yes. It was within that compressed file, p.rar.
Q And what kind of software was it?
A The JeRM is software needed to communicate with the MSR206, for example. That allows an individual to actually write dumps, or data, to the magnetic stripe found on the back of, say, a gift card. So it's how you interface, or talk, to the hardware of the MSR206.
Q Okay. Now, if you could read this bottom paragraph.
A "What is this program? It's a utility program I wrote to interface with the MSR206 mag stripe reader/writer. Why did I

write it? I wasn't satisfied with the quality of other programs I tried. I made this program to solve the problems I was having with the other programs. I tried to design it to be very quick, easy, and" -- it's kind of cut off -- "efficient to use. But at the same time, I want it to be very comprehensive so that you would never have to load up another program to use a function that I didn't include. I plan to keep adding more features too. Although I tried to make the program very easy to use, there are some things that are not self-explanatory. That's what this README file is for. I'll try to explain every feature of the program so you'll have no problems using it."

Q We're going to the sixth page.

What is this information on Page 6?

A Discusses setting up and how to actually use the JeRM to communicate with a mag stripe reader, such as MSR206.

Q And at the bottom of the page, what does it say?

A "After you connect MSR206, you can copy Track 1 and Track 2 that buy bought already at 2Pac.cc shop, and click 'write' and slide our gift card through MSR206."

Q It looks like the second page -- is that some of the same text we just looked at?

A It is.

Q And then what's the last thing saying?

A "Finish. Clone of card and ready for use. You can use at any shop (POS)."

Q Is this process of generating fraudulent credit cards consistent with how you've seen it practiced out in the field?
A Yes.
Q Based on your review of that file, did you develop an opinion as to what it was intended for, or what purpose it could serve?
A Yes.
Q And what was that opinion?
A Well, one, due to the links and ads on there, appeared to want to direct users to buy dumps from 2Pac.cc. And then also, it was a tutorial for users to learn how to actually purchase the dumps and then put those dumps to manufacture a counterfeit credit card.
Q Did you have an opinion or a suspicion about how that would actually be communicated, in other words, how that information would be shown to the world?
A Yes.
Q And what means would that be?
A That would be a website.
Q Did you go online and search to determine whether there was a website out there on the web containing this text?
A Yes.
Q And what did you find?
A I found a site, posdumps.com, which contained that content.

Q Did you do anything to capture or memorialize what you saw?
A Yes. I used software to clone the site, essentially made an offline copy so that could be viewed offline. You wouldn't have to go on the internet anymore to see it.
Q Can you tell us what Exhibit 11.2 is?
A That is the cloned copy of posdumps.com which I obtained.
Q Is this an actual live website that we're looking at?
A No. No. It's a copy of that -- what that site was like at that time.
Q Is it an accurate representation of what the website looked like at that time?
A Yes.

MR. WILKINSON: Government offers 11.2.

MS. SCANLAN: No objection.

THE COURT: 11.2 is admitted.

(Exhibit 11.2 was admitted)

THE COURT: Counsel, before you begin, let's let the jury have a stretch break.

Please be seated.

Counsel, you may continue your direct examination.

MR. WILKINSON: Thank you, Your Honor.

BY MR. WILKINSON
Q How did the content of this live website compare to that RAR file that you found on the defendant's laptop?

A It appeared to be very, very similar, but with a few additions.
Q Can you please read the text -- the first paragraph at the top of the screen?
A "This is tutorial how to buy dumps and use in store (POS). Make and using fake credit card. Here I explain you how to earn money from $500 to $50,000, or even $500,000. Remember, this is illegal way. Process from the start to the finish." And then there's a link for 2Pac.cc, as well as an ad.
Q Same ad that you found on the defendant's desktop?
A Yes.
Q Now we've got a table of contents here.
How many items on the table of contents were on the defendant's laptop?
A Four.
Q Okay. Were they the same first four listed here?
A Yes.
Q Okay. So are there additions here?
A Yes.
Q And what are those?
A Five and six. Five is a hint on "how to find zip for our dump." And six is a hint on "how to get balance for our Discover card dump."
Q We'll scroll down the website.
Are we looking at essentially the same text that you just

read and walked us through a minute ago?
A Yes.
Q Same image of an MSR206 that was on defendant's laptop?
A Yes.
Q Same image of the blank credit cards that was on the defendant's laptop?
A Yes.
Q And are we looking now at the same three methods of selecting dumps on the 2Pac website, that you walked us through?
A Yes.
Q The section on how to generate Track 1 and why this is needed?
A Yes.
Q Also the same as the text on the defendant's laptop?
A Yes.
Q Now what section are we looking at?
A Section for writing dumps on plastic and the discussion of the software, the JeRM.
Q Also substantially the same as what was on the defendant's laptop?
A Yes.
Q Now, you mentioned that there was some new content on here.
Have we gotten to that yet?

A Yes.
Q Okay. And what's the title of the new content?
A "Some hint to find a zip code for USA dumps private method."
Q Okay. And what is this a tutorial on?
A How to find a zip for a dump, in particular because for some transactions to be successful, you need the zip code for the card.
Q And how does he explain how to go about doing that here?
A Talks about sites you can go to to research an individual and potentially get an address which would provide a zip code.
Q Have we moved on to the next new section on this website?
A Yes.
Q And what's this one about?
A "Some hints for Discover card dumps to get available balance."
Q Okay. Why don't you go ahead and read this section, please.
A "First we need to buy dumps with original Track 1 plus Track 2 at shop 2Pac.cc." It shows an example of a dump which would have been purchased. "We need to search SSN (Social Security number) and zip for name. First name Talene, last name McCarthy, middle name "K," in all states of U.S. Because name is long and rare, there may be one to five variants of different peoples with different SSN."

Q And let me just stop you there. It looks like he's talking about how to find an SSN.

Is that needed to determine the amount of balance on a Discover card?

A Yes, it could be.

Q And why would someone with a fraudulent credit card want to know the available balance on that card?

A So you'd know how much you could spend on the card.

Q Does it go on to provide tips on researching people with SSNs, as we scroll down?

A Yes.

Q Are we at the bottom of the website now?

A "PS, with this information, you have chance to get a PIN. Like you can find a phone number of cardholder at www.address.com. And if you fluent in English language, you can call holder and say that you from Discover and say your last transaction was in supermarket for $19.99, and your" -- typo -- "for available balance is $19,916. And to approve that transaction, you need a PIN number, or some another story."

Q And what's the intent of going -- what would this cause the people at Discover to provide?

A Potentially reveal the PIN or information that was sought.

Q Did you -- after capturing the website and reviewing it, did you do research into the registration information for that website?

A Yes.
Q Is Exhibit 4.7 the DomainTools report showing that information?
A Yes.
MR. WILKINSON: The government offers 4.7.
MS. SCANLAN: No objection.
THE COURT: 4.7 is admitted.
(Exhibit 4.7 was admitted)
BY MR. WILKINSON
Q And we're going to scroll down to the fourth page.
So do we have the domain name that's being registered listed on here?
A Yes. Posdumps.com.
Q And when you look at registration information, what piece of information are you most interested in?
A The e-mail address, that's typically the most valid information. In this case, it was jchow@bk.ru.
One other useful piece of information was the creation date, which can be seen, of June 3, 2014. That's relevant, is that matches the creation date of that p.rar file, which was found on the desktop -- or found on the defendant's laptop.
Q So could you explain that one more time, why that was significant?
A Sure. The creation date for the domain being registered on the internet, of June 3, 2014, that registration date

matched the date that the file p.rar, containing all the information we just reviewed, was created on the defendant's laptop.

Q Did you also research registration information for the website 2Pac?

A Yes.

Q Is Exhibit 4.6 the DomainTools report that you came up with?

A Yes.

MR. WILKINSON: Government offers 4.6.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 4.6 was admitted)

BY MR. WILKINSON

Q And we're going to go to the 34th page of that exhibit.

Is that the registration information? Are we looking -- the screen on the right, are we looking at the registration information for the 2Pac site?

A Yes.

Q And does it list a domain name, at the top there?

A It does; 2Pac.cc.

Q And the registrant e-mail?

A Jchow@bk.ru, which is the same registration address used for posdumps.com.

Q And did the fact that the registration information for

posdumps and the 2Pac website matched, was that significant to you, as an investigator?

A Yes. It appeared that the same person was responsible for both sites.

Q Exhibit 13.12, is that one of the documents that you found on the computer?

A Yes.

Q And, first of all, what type of file is it?

A A text file.

Q And what about the content of the file? What kind of things are contained within the file?

A Usernames and passwords for a variety of websites and accounts. In particular, it appeared that most of the websites related to carding, and that the credentials for accounts appeared to be mainly for, like, digital currency.

Q Did some of the passwords appear to be randomly generated?

A Yes, some did.

Q And were there also some that were user generated?

A Appeared to be.

Q Were there particular passwords or logins that appeared in here that you'd seen elsewhere in the investigation?

A Yes.

Q And can you tell us the most significant of those?

A Yes. So --

MS. SCANLAN: Your Honor, I object.

Can we offer the exhibit first, before he testifies about what's in it?

THE COURT: Was he establishing foundation or substantive testimony, Counsel?

MR. WILKINSON: It was substantive testimony, Your Honor.

THE COURT: All right. Let's offer the exhibit, Counsel.

MR. WILKINSON: Okay. The government offers 13.12.

THE COURT: Any objection?

MS. SCANLAN: May I inquire?

THE COURT: Yes.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Agent Fischlin, I may have missed it -- and I apologize -- where did this come from?

A From the defendant's laptop.

Q In what file source?

A I can't remember the exact path. It was in one of the folders on the laptop.

Q Do you know what kind of folder?

A I know it was a general folder on the laptop.

Q And is this a text file?

A Yes.

Q Do you know if it was in one of the internet browser

folders, or what kind of -- where was it?
A I recall it was not in an internet browser-type folder. I do recall that much.
Q Okay. What kind of folder was it in?
A A folder on the computer that could be created by a user.
Q I'm sorry. That could be created by the user?
A Yes.
Q So you don't know if it's created by the user?
A It -- the exact folder, I can't remember what it was called. I know it wasn't found in a portion where the internet would have just stored it.

MS. SCANLAN: Based on that, I don't -- I'm going to object to this. I don't think this is an admission of a party opponent if we can't establish that it was created by the user of the laptop.

THE COURT: I think sufficient foundation has been established by the fact that the witness has testified it was found on the computer that was seized from the defendant.

Objection is overruled. 13.12 is admitted.

Please continue.

(Exhibit 13.12 was admitted)

DIRECT EXAMINATION

BY MR. WILKINSON

Q Before we get into it, before we look at the document, I think I was asking you whether there were specific passwords

that came up repeatedly.
A Yes.
Q And what were some of those passwords?
A Several times; a password -- or variations of the password "ochko123."
Q Okay. Was there another one, a username or password that came up frequently?
A Yes. "Smaus" popped up numerous times within this document.
Q Displaying 13.12, does this -- are portions of this document in Russian?
A Yes.
Q Was that sent out to get an English translation of those Russian portions?
A Yes.
Q Displaying 13.12C, which has been previously admitted, is that the version with the Russian translated into English?
A Yes.
Q And how is it notated? How can you tell which parts have been translated?
A The portions in bold.
Q So why don't you walk us through this page and tell us what items you saw here of significance.
A So there are a variety of items of interest in the document. Up top, we can see a URL, or web address. In

particular, that web address for a carding forum was only available through Tor. That can be notated by the ".onion" address. After that, we can see throughout the document references to username "2Pac" or "2Pac.cc," and then use of the password "ochko123," for example. Some of that's been highlighted within this document.

Q What do you see below that?

A A website, posdumps.com.

Q And then what do you see below? What's the next highlighted item there?

A It's a new password for the shop. And then there's a long password, because it appeared to have been computer generated.

Q Skip to the fourth page of this exhibit.

What items of significance did you see here?

A Yes. The use of an e-mail address and maybe for some type of login the password "smaus123." Again, "smaus" was a nickname that previous investigators associated with the defendant. A login of "2paccc" and the name "James Chow" again --

Q Let me stop you right there.

Did you recognize "James Chow" from anywhere?

A Yes.

Q And where was that?

A The domain 2Pac.cc had been registered with the e-mail jchow@bk.ru.

Q Is that an e-mail right below there?
A It is. That e-mail had also been used to register posdumps.com.
Q And then what do we see at the bottom, which is highlighted?
A An eBay user ID of "selez_roma."
Q And is that of significance to you in any way?
A It's a portion of the defendant's name.
Q Let's go to the fifth page.
What do we see here?
A More use of the e-mail address jchow@bk.ru, which again was used to register several domains of interest. More use of the password ochko123; in this case, there was an "S" added to the end of it. It's a variation of that password. Near the bottom, again, login of "2paccc," more use of the name "James Chow," and that e-mail address, jchow@bk.ru.
Q Move along to Page 9 of the exhibit, what do we see here?
A There's one section showing the ten most-used personal identification numbers. There's a list of that.
Q And let me ask you there, in your training and experience, is it useful for people in the carding industry to know frequently used personal identification numbers?
A It can be.
Q And why is that?
A For access for the card.

Q Please continue.
A Again, throughout this document, more use of that password, ochko, ochko123, variations of it. Also highlighted there is an e-mail address, davydov.alexei@mail.ru. And previous investigators had seen that one of the domains of interest, it was on track2.name, had been registered under the name "Alexey Davydov."
Q Why don't we just pull that up. 4.12 has been previously admitted as a summary of the track2.name website.
Do you see alexei.davydov there?
A I see "Alexey Davydov" as a name for the registrant.
Q We're on to Page 10 of the document.
What's the first item you see here?
A 2Pac.cc, more use of that.
Q And do you know what crimes.ws is?
A I personally do not.
Q What about the next item?
A Login credentials for the site inFrauD.cc, in this case a login name of 2Pac. InFrauD was a carding forum where users can go to discuss aspects of carding.
Q And what would having credentials for 2Pac allow you to do on the inFrauD website?
A Allow you to log in, view content, post, just have access to the site.
Q And moving down, can you tell us what the next highlighted

item is?
A There's 2Pac.cc, and then there appears to be a password of smaus123 for verified.cm, that specific domain, again another carding forum where users can go to discuss carding.
Q And then the last highlighted item at the bottom?
A Again, more use of the nic 2Pac. And then in particular, this portion appears to be discussing a banner and how much it would cost for a banner to be placed.
Q What is a "banner"?
A It would be an ad, kind of like we saw earlier on the defendant's laptop, that running ad. That would be a banner.
Q We're on to Page 11.
Can you tell us what items you saw here?
A Again, it appeared to be more use of a login of 2Pac; the password involving smaus, in this case, smaus123; various times smaus with some extra characters added to the end of it. That one was for MtGox, which was a Bitcoin exchange at the time -- or in the past.
Q And was Bitcoin used in any of the websites that you were investigating here?
A It was an accepted form of payment on 2Pac.cc.
Q And please continue.
A More login credentials involving 2Pac, the name James Chow, and the e-mail address jchow@bk.ru.
Q And just remind us one more time, for jchow, what

address -- what websites was that address used to register?
A Both 2Pac.cc and posdumps.com.
Q On to Page 12, what is the first item that's highlighted on here?
A It's a web address for PACER. And under that appears to be login credentials for PACER. It is a site maintained by the U.S. Courts, where individuals can look up federal cases.
Q Is that a website that you've used?
A I personally have not, but I am aware of it.
Q And what kinds of things are stored on the PACER website?
A Information about federal cases, even criminal cases. You could see, for example, indictments, that sort of information.
Q What's the item below that?
A A Liberty Reserve account number.
Q And the next item down?
A Perfect Money account number. And under that, a password involving smaus and some extra characters added to the end of that.
Q What is Perfect Money?
A It's a form of digital currency. It was an accepted form of payment on 2Pac.cc.
Q And then at the bottom, there are two more items highlighted down here.
What's this?
A It appears to be, again, more credentials, jchow and a

potential password of smaus123, username of "administrator."
Q Does "administrator" have a use or meaning in computer administration circles?
A Yes. Administrator would have the highest level of privileges on a computer.
Q We're onto Page 13.
What are the top two highlighted items there?
A Top two is WebNames.ru, and then login credentials for it of jchow. And then there's a password there. And to the far right, you can see those login credentials are "(for 2Pac.ccdomain)."
It should be noted that WebNames.ru is the same as the registrar "regtime." So this would have been where you'd go to actually register the domain. For example, 2Pac.cc, you'd have to go through WebNames.ru. So it appeared to be login credentials to do that for the 2Pac domain.
Q And then the next item down here?
A More, appeared to be, use of a username of 2Pac. Near the bottom, you can see that there's a reference to bulba.cc, which again was a dumps shop investigated by previous investigators. Under that, there's an e-mail of bulbacc@yahoo.com, which was used to register that domain, bulba.cc.
Q And is there a username and password for bulbacc, as well?
A It appears to be. Bulbacc, it appears to be a password for it. And then right above that, you can see kind of what I

referenced earlier. Regtime.net, it is also WebNames.ru. So that's where you go to register, you know, domains for regtime, through regtime.

Q And displaying on the left Exhibit 7.3, which was admitted this morning, it's a registration e-mail for the bulba website.

Can you tell us what the login and password were for that website?

A Bulbacc is the login. The password is telkom135. And those match what was found within the credentials file on the laptop.

Q And going back to Exhibit 17.7, can you show us, using your finger, which e-mail account on here these credentials are for?

A Could you rephrase that question?

Q Sure. So we were just looking at the login for the bulbacc e-mail account.

Can you show us where that e-mail account appears on Exhibit 17.7?

A Sure (indicating).

Q Okay. Let me back up for a second. Then at the bottom of this page, we have a number starting with a "U."

In your training and experience, does that type of number look familiar?

A Yes. I know that is a Liberty Reserve account number.

Q And the name associated with it?

A Salitov.maxim.
Q And then putting up Exhibit 9.11, which was previously admitted as the summary of the Liberty Reserve accounts, does one of those accounts have that salitov.maxim web e-mail address?
A Yes.
Q Okay. And the total amount of proceeds that were deposited into that account?
A It appears to be approximately $6.8 million.
Q Can you tell us what a "cached web page" is?
A Sure. So when a user visits a website, a computer can cache fragments of that website, so when a user goes back, it will load faster. So some of that content can be temporarily stored on a user's computer. That's what a cached website would be.
Q How are cached -- reviewing cached websites useful to you in your investigations?
A Well, with cached web pages, you can actually see a page much like the user did when they saw it on the internet.
Q Okay. What does reviewing cached web pages tell you about the user's activity?
A Well, for one, that the site's been visited. And two, it gives a nice visual, because you see it much like the user did.
Q And as part of Agent Mills' forensic exam of the laptop, did you ask him to look at cached web pages?

A Yes. He was asked to look for internet history.
Q And did he come up with some that was interesting to you?
A Yes.
Q Is Exhibit 13.16 one of those cached web pages that Agent Mills identified on the web -- on the computer?
A Yes.
Q And can you tell us, generally speaking, what it is?
A It involved essentially a Whois search for the domain 2Pac.cc, to see what was publicly available about the site and how much traffic it may have been receiving.
Q Is Exhibit 13.16 an accurate representation of what that file looked like?
A Yes.

MR. WILKINSON: The government offers 13.16.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.16 was admitted)

BY MR. WILKINSON
Q Okay. So now that the jury can see this, can you explain what it is?
A Yes. Again, a Whois-type search on 2Pac.cc. You see what information was publicly available, and also can give up statistical information for the site.
Q What kind of statistical information?

A Where it's ranking, and potentially traffic.
Q In your training and experience, who -- why would -- who would be interested in the ranking of a particular website and its traffic levels?
A An owner of the site, to make sure it's being seen and visited.
Q And we see here that it mentions Cloudflare and has an IP address.
Is this related to something you were explaining earlier?
A Yes. The domain 2Pac.cc was protected by Cloudflare for DDoS protection. Again, so if you're doing a lookup of that site, you wouldn't see the true IP address, but you'd see Cloudflare's IP address, which is what you can see within this cached web page.
Q So if I were publicly researching the 2Pac website, is this the IP address I would come up with?
A Yes.
Q Did you find similar research activities, or evidence of similar research activities, for the posdumps website?
A Yes.
Q And is Exhibit 13.14 another one of these cached web pages?
A Yes.
Q And is this an accurate representation of what it looked like on the computer?

A Yes.

MR. WILKINSON: The government offers 13.14.

MS. SCANLAN: No objection.

THE COURT: 13.14 is admitted.

(Exhibit 13.14 was admitted)

BY MR. WILKINSON

Q So what are we looking at here?

A Cached web page; in particular, the search was related to posdumps.com. And it contained statistical information for the site, how many visits it had received during a time period, that type of information.

Q Can you tell when the search was run?

A It looked like on or about July 3, 2014.

Q Now, if we look down here, it shows via -- there's a summary, and it says "reported traffic."

Is this for a particular period of time?

A Yes, for the month of July 2014.

Q And what statistics does it provide about July?

A How many times a site's been visited, how many unique or different visitors there's been to that site, and then how much traffic or bandwidth that was taking up.

Q How many times was it visited?

A Number of visits would be 268, with 230 of those being unique visitors, or different visitors.

Q And then scrolling further down, we see "monthly history."

And it looks like there's nothing, and then all of a sudden there's bars that come up.

How do you interpret that statistic?

A Sure. It shows that the site wasn't active before that time. And again, a Whois search revealed the domain was created on June 3, 2014.

Q So is that why there's no traffic in May?

A Correct.

Q And then down here, does it provide additional statistics on visitors?

A Yes.

Q And do you know why these numbers are bigger than the ones we just looked at?

A Sure. The time period we just looked at was for three days, whereas before that, for June, you can see it's for that month. So that's why there would be a larger data set.

Q How many visits were paid to posdumps during its first month on the web?

A Approximately 4,500, with approximately 3,400 of those being unique or different visitors.

Q Is Exhibit 13.18 another piece of cached web history from the computer?

A Yes.

Q And is it an accurate representation of what it looked like on the computer?

A Yes.

MR. WILKINSON: Government offers 13.18.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.18 was admitted)

THE COURT: Counsel, this will be the last exhibit before the lunch break.

MR. WILKINSON: Yes, Your Honor.

BY MR. WILKINSON

Q What web page are we looking at here?

A Omerta, which was a carding forum.

Q And what do we see here in the middle of the web page?

A That is the ad for 2Pac.cc, the same one that we saw on the defendant's laptop.

Q And scrolling to the lower right-hand corner, can you tell who -- let me back up.

To get onto the Omerta web page, do you need to log in?

A Yes.

Q Do you need to log in a password for that?

A Yes.

Q And would that associate you with a particular user on the Omerta web page?

A Yes.

Q And so was the person who was viewing this website on Mr. Seleznev's computer logged in?

A Yes.
Q And who was he logged in as?
A As 2Pac.
MR. WILKINSON: Okay. I think that's a good place to break, Your Honor.
THE COURT: Members of the jury, we'll take our afternoon recess at this time.
(Jury exits the courtroom)
THE COURT: Counsel for the government, where are we by way of finishing today? You indicated yesterday the possibility of either finishing early, or having enough witnesses. So what's the status?
MR. WILKINSON: Your Honor, I probably have an hour and a half left with this witness. And we do not intend to put another witness on after.
THE COURT: So do you think you'll fill up the entirety of the day?
MR. WILKINSON: So my intention would be probably to go until about the afternoon break and be done. I don't know what the defense has in mind for cross examination.
THE COURT: All right. And then in terms of your projections on completion of the government's case in chief, are we still talking about Tuesday?
MR. WILKINSON: Tuesday morning.
THE COURT: Okay. And Counsel, on that -- one other

thing on Exhibit 11.2. There was testimony about that being a tutorial. And that makes reference to Talene McCarthy. That exhibit provides the name, address, and Social Security. I don't know if that's a fictitious person or a real person. I suspect it was a real person. The Court has concern of that person and any other person's private information, that degree of information, that would be available downstream.

So are there any protections that the government can ensure by way of redaction, or anything else, so that we don't have that problem?

MR. WILKINSON: Yes, Your Honor.

THE COURT: All right. So I'll direct the government to make sure, on that particular exhibit and any other exhibit, assuming there's no defense objection, that we at least eliminate the Social Security number.

Any objection by the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: So to the extent any exhibit's already come in with that type of information, make the proper redaction.

MR. WILKINSON: Yes, Your Honor. Understood.

THE COURT: Anything else to take up, by counsel for the government?

MR. WILKINSON: Yes. One thing, Your Honor.

THE COURT: You may be seated, Counsel.

MR. BARBOSA: One matter we've discussed with defense counsel is, for next week, whether or not the government's expert may be in the courtroom for defense expert's testimony. We had indicated, in our response to the motion to exclude witnesses, that we would request an exception for experts. I believe that was practiced during the suppression hearing, and I think it would be appropriate during this hearing too.

THE COURT: Is there any objection by the defense?

MR. BARBOSA: Yes.

MS. SCANLAN: I do have an objection, but I didn't just look at whatever they put in their trial brief about it.

I would object to their expert being present, their rebuttal expert, potential rebuttal expert being present when our expert is testifying on direct.

THE COURT: Let me ask this, is there going to be reciprocation, Counsel, where the defense expert would be permitted to be in court --

MR. BARBOSA: Absolutely. Yes.

THE COURT: Do you wish to revisit that now, Counsel?

MS. SCANLAN: No. Because we talked about this -- because the idea that we're proposing is that our expert can be here when their rebuttal expert testifies, but all their other experts already testified. So it's not really -- this isn't really a fair trade.

THE COURT: And, Counsel, any particular

justification to have your witness present -- suppression hearing is different, as opposed to trial testimony.

MR. BARBOSA: For this particular expert, the testimony is rebuttal testimony specific to the defense expert, so it's not regarding carding or other matters that have been addressed by the expert witnesses. So I think, especially in light of the history already, that both experts have sat in for each other's prior testimony. They've read each other's reports. It would seem to be fairly standard practice in a situation like this.

THE COURT: It may be standard practice, but I think it was done in the prior proceedings by way of courtesy allowance, as opposed to a procedural, statutory, or rule requirement.

So absent the same, the Court will sustain the objection. Your expert will not be permitted to remain in the courtroom while he's testifying, and the Court will adhere to its rule on the exclusion of witnesses.

Anything else to take up, by counsel for the government?

MR. BARBOSA: No, Your Honor.

THE COURT: Defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Have a good lunch. See you after lunch.

(Recess)

THE COURT: Counsel, you may continue your direct

examination.

MR. WILKINSON: Thank you, Your Honor.

BY MR. WILKINSON

Q Welcome back, Inspector Fischlin.

A Thank you.

Q When we left off, I think you were talking about some of the cached web pages that you found on Mr. Seleznev's computer.

Is Exhibit 13.17 another one of these cached web pages?

A Yes.

Q And is it a true and accurate copy of the file as it appeared on the computer?

A Yes.

MR. WILKINSON: The government offers 13.17.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.17 was admitted)

BY MR. WILKINSON

Q What website are we looking at?

A InFrauD.

Q Okay. And what is inFrauD?

A Carding forum where users can discuss various aspects of carding.

Q We heard about the carder.su forum and the Omerta forum.

Is it similar to those types of forums?

A Generally, yes.

Q And does inFrauD require someone to input user information to log on?
A Yes, you need to log on.
Q And can you tell from this web page, or this fragment, whether the user of Mr. Seleznev's computer was logged on to the inFrauD website?
A Yes. The user was logged on as 2Pac. And again, pointing back to that user credential file we looked at, there was credentials for inFrauD within that file, as well.
Q And what do you see on the screen that shows you that he was logged in as 2Pac?
A Well, a few lines down from the top you can see, "Welcome, 2Pac."
Q Right where I highlighted?
A Yes.
Q Is Exhibit 13.20 another of the cached web pages that was found on the computer?
A Yes.
Q And is it an accurate copy of the file as it looked on the computer?
A Yes.
Q And what's the website that it's depicting here?
A PACER.
Q Okay. And I think you mentioned PACER once before, but can you refresh us on what the PACER website is?

A It's maintained by the U.S. Courts, and it's a site where users can go to look up federal cases, even criminal cases.

MR. WILKINSON: The government offers 13.20.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.20 was admitted)

BY MR. WILKINSON

Q So we have the "PACER" title at the top.

What do we have just to the right of that? What is it saying?

A "Criminal party search."

Q And what is that indicating here?

A You're looking for criminal records.

Q And who, specifically, was looking for criminal records?

A The user logged in was gh0024. And again, within that user credential, or cheat sheet file, we found there was a user credential for this site.

Q And so it would have been -- just to back up a little bit, it would have been -- was it the user of Mr. Seleznev's computer that was looking at this website?

A Yes.

Q And you mentioned the username. What is that again?

A Gh0024.

Q And I'm pulling up Exhibit 13.12C.

Can you remind us what that exhibit was?

A That was the user credential, or cheat sheet, text file.
Q Where was it found?
A It was found on the defendant's laptop.
Q And do you see that "Gh024" [sic] on there?
A Yes, I do.
Q And what website is it talking about?
A PACER.
Q So the user was doing a criminal party search.
Can you tell us what name the party was searching for?
A Yes. For this search, it was "Selez," which is a portion of the defendant's last name.
Q Is that right where I'm highlighting?
A Yes.
Q And what was the date when this search was conducted?
A July 3 of 2014.
Q And how did that compare in time to the date of the defendant's arrest?
A It was two days prior.
Q We're scrolling down to the second page.
Is this another criminal party search?
A Yes.
Q Same date?
A Yes.
Q And what was the name that was searched for here?
A 2Pac.

Q And going to the third page, another criminal party search?
A Yes.
Q And what name did the user search?
A Bulba, which again was a nickname that previous investigators had associated with the defendant.
Q Calling up Exhibit 13.19, is this another file that was found on the defendant's laptop?
A Yes.
Q And what type of file was it? What format?
A This was a graphic file.
Q Like, a photograph?
A Like, a screenshot.
Q Okay. And is this an accurate replication of that screenshot?
A Yes.

MR. WILKINSON: The government offers 13.19.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.19 was admitted)

BY MR. WILKINSON
Q What is the website we're looking at here?
A Try2Check.me.
Q And what is Try2Check.me?
A It was a site that acted as a checker service. You could

run a card through that site and determine if it was valid, if it was good.

Q Was this a website that you needed to log on to use?

A Yes.

Q And was there a user logged on to the site?

A Yes, as 2Pac.

Q Is that the place I'm highlighting right here?

A Yes.

Q And down below, what are we looking at here, in the left-hand part of the screen?

A A card number that had been run through the service.

Q So is that an example of a card that would be checked on that service?

A Yes.

Q Okay. Let's move on to another topic now. I want to ask you about parsed search terms.

Can you tell the jury what a "parsed search term" is?

A Sure. Those are search terms that have been entered into search engines on the internet.

Q And did you ask Special Agent Mills to look for parsed search terms in this investigation?

A Yes. That would be part of the internet history search.

Q And so where would these parsed search terms originate from? In other words, who would have entered them into the computer?

A A user of the computer.
Q What is Exhibit 13.30?
A Some of the search terms that were obtained from the laptop. These are just -- these are just some of them, not all of the search terms that were recovered.
Q Is this an accurate list of data that was taken from the computer and copied onto this sheet?
A Yes.

MR. WILKINSON: The government offers 13.30.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.30 was admitted)

BY MR. WILKINSON
Q So let's just focus in on this top one, just to get a sense of what's going on here.

Can you just walk us across the column? And I'll scroll it over in a minute. But tell us what each of these columns is for.
A Sure. The record, that's just provided by the program, so that's nothing from the laptop itself. The search term is the search term that was entered into the browser. In particular, this was Google, so the search term, in parentheses, "Omerta.cc" was entered.
Q And when you say it was entered, it was entered --
A Typed in.

Q By?
A A user of the computer.
Q Okay. And sorry, I interrupted you.
So it was typed into Google?
A Yes.
Q And then what about where it says "web page title"?
A That would be the title of the web page.
Q Okay. So let's start to walk down these a little bit.
Well, first let me ask you --
THE COURT: Members of the jury, can you see that? Would it help to enhance it at all?
JUROR: It would.
THE COURT: Counsel, perhaps you can enhance it.
MR. WILKINSON: Yes, Your Honor.
BY MR. WILKINSON
Q First, let me ask you, how do parsed search terms help you in an investigation?
A Well, it gives you an idea of the user's online internet habits and their interests. So these are terms entered into internet browsers --
Q Okay.
A -- internet search engines, via browsers.
Q So you mentioned that the first one was "Omerta."
Can you remind us what Omerta is?
A It is a carding forum.

Q And what about -- what's the one -- the search term in the second row?
A Rescator.so.
Q What is "rescator"?
A Rescator is known as a hacker in the community. In particular, he's been affiliated with some major data breaches.
Q And what about the next one down?
A The search term, in parentheses, "Roman Seleznev" was entered into Google.
Q And why did you select that as an entry of interest?
A It's the defendant's name.
Q And what does that show you, the fact that the defendant -- or the fact that the defendant's name is in there?
A That there was an interest in what was publicly available by entering that search term into a search engine.
Q What about the next one down?
A "2Pac.cc." That was entered into search engine Google.
Q And the next one?
A There's an IP address, followed by "2Pac," which was entered in the search engine Google. In particular, that was the IP address for the domain 2Pac.cc, which was not available to the public.
Q What was the next one down?
A "Buy dumps." That was entered into Google.
Q And the next one?

A "CarderPlanet." That was entered into Google.
Q What is CarderPlanet?
A It was either a dump shop or carding forum. I can't remember which one it was, exactly. But it was related to carding, nonetheless.
Q And the next one down?
A "Dumps shop." And that was entered into Google.
Q Next?
A "MSR206." That was entered into Google.
Q Next one?
A "Posdumps.com." That was entered into Google.
Q Next one?
A "Sell dumps." That was entered into Google.
Q And the last one?
A "Site:2Pac.cc." And that was entered into Bing.
Q And what does this "site:2Pac.cc" mean? What does that search entry call up?
A It's more of an advanced operator, to narrow search results for the site you're looking at. So it would just limit the hits for the 2Pac.cc. It's a narrowed search.
Q And it narrows it to the 2Pac website?
A Correct.
Q Okay. And it looks like there are two more on here.
What's the next one?
A "track2 bulba." That was entered into Google. And again,

both of those are nicknames that previous investigators associated with the defendant.

Q And the last one?

A "Writing dumps on plastic." And that was entered into Google.

Q And what does "writing dumps on plastic" mean?

A That's the process of actually writing credit card track data to the magnetic stripe found on the back of a plastic card, such as a gift card.

Q What is "form history"?

A That is data entered in the forms on websites. A good example would be, when you go to a site to maybe book a flight, a hotel room, what have you, there will be certain fields, or input fields, such as you'll have to fill out your name, first name, last name, maybe your address, maybe a credit card number. And those are fields that you're entering data into.

Certain web browsers, such as Firefox, depending on your settings, can capture and save that data. And it can work as an auto complete. So if you have to enter -- if you're asked for a similar input field, it can kind of complete it for you, if you wish. It's convenience.

Q And did Agent Mills look for Firefox form history as part of his investigation?

A He did. That was part of the internet search, internet history search.

Q Okay. And what was -- for what purpose? What was he looking for?
A Again, to see -- form history can show what data a user has actually entered into these input fields on web pages, so it could help with dominion and control and maybe even the user's interests.
Q Is Exhibit 13.31 a compilation of the form history for Mr. Seleznev's computer?
A Yes, that's some of it.
Q Does it accurately reflect data that was copied off of that computer, onto this exhibit?
A Yes.
MR. WILKINSON: Government offers 13.31.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 13.31 was admitted)
BY MR. WILKINSON
Q So let's walk down this one again.
What does the "field name" column represent here?
A Sure. So below that are the names of the input fields that were on those forms on the web pages.
Q So does that mean that's what the web page is asking you to type in?
A Yes.
Q And then what is "value"?

A That would be what the user entered. In this first case, that is a date of birth. And it does match the defendant's date of birth, what was found on the passports in his possession when he was apprehended.
Q What do we have -- in the second column, what information was the user of Mr. Seleznev's computer asked to input?
A A passport number. And the passport number listed there matches the number found on one of the passports in his possession when he was apprehended.
Q And when you say one of the passports, is that his international passport?
A Correct, his international.
Q Okay. What about contact -- or what about the third column? What's the field here?
A "Contact e-mail."
Q And what did he type in to fill in that column?
A Romariogro1@mail.ru.
Q Is that an e-mail address you've seen elsewhere in the investigation?
A Yes. For one, it was found on documents in his possession when he was apprehended. And it was also found on the HopOne server. In particular, it was a travel reservation, or order. It was found on one of those.
Q "Doc number," I think we already covered that.
Is that the passport number again?

A Yes.
Q And then the e-mail, same e-mail address, romariogro?
A Yes.
Q What about the next place he was asked to enter an e-mail?
A The e-mail entered was jchow@bk.ru. Again, that e-mail address was used to register both posdumps.com and 2Pac.cc. And that e-mail address was repeatedly seen within that cheat sheet, or user credential file, which we discussed a little bit ago.
Q Okay. The next column has a field name for first name.
And in this case, what did the user enter as a first name?
A "Roman," which is the defendant's first name.
Q What about the next time the defendant was asked to enter a name?
A It was an input name, and the value entered was "James Chow."
Q And where else has the "James Chow" name come up in your investigation?
A An e-mail address for that name was, again, found to be registered at posdumps and 2Pac.cc. And that name popped up a few times within that user credential, or cheat sheet file.
Q Okay. Now we're on to a last name.
What last name was entered on this next line?
A "Seleznev," which is the defendant's last name.
Q And we see the romariogro e-mail. We'll skip over that.

What's the next one down there that's -- one that says "Entry 249"?

A It's a login field. And the value entered was "2Pac." Again, 2Pac is a nickname associated with the defendant. Domain 2Pac.cc popped up during the investigation. And that username, 2Pac, was seen numerous times within that user credential file.

Q So what does this event indicate that the user of defendant's computer was doing?

A Used it to log in to a site.

Q As?

A 2Pac.

Q What about the next login?

A The value entered was "jchow." That was used to log in to a site. And again, the e-mail address affiliated with that was used to register posdumps.com and 2Pac.cc.

Q What about Item 2335?

A The input field was "street," and the value entered was "Ostryakova 26-113." That address matches what was listed on the -- one of the defendant's passports.

Q Okay. And was that also an address that turned up in several places on the criminal infrastructure?

A Yes. Previous investigators had seen that address before.

Q And then the last two?

A A username of "2Pac" was entered. And then the last one,

a username of "jchow@bk.ru" was entered.
Q Do you recognize Exhibit 13.46?
A Yes.
Q What is it?
A Those are stored usernames and password that were within the internet browser Firefox, on the computer.
Q How does this compare to the other browser information that we've looked at?
A Well, this contains specific usernames and passwords for specific sites.
Q So it tells you which site and which password was entered in?
A Correct, which ones were saved by the browser.
Q And is this an accurate replication of the information that was found on the defendant's laptop?
A Yes.

MR. WILKINSON: The government offers 13.46.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.46 was admitted)

BY MR. WILKINSON
Q What do we see here on the first item? What is the website that the user visited?
A 2Pac.cc.
Q And the user's name?

A "Admin."
Q In your training and experience, what does "admin" mean on a website?
A It means they have the highest of level control of the computer site, in general.
Q Scroll down. Actually, go to the next page.
The top of the second page, what website had been logged on to?
A Verified.cm.
Q Do you know what that is?
A A carding forum.
Q And how had the user of defendant's computer logged on, what username?
A Username of "2Pac.cc."
Q And a password?
A "Smaus123."
Q What about the next entry down, what website did the user log on to?
A Vpro.su.
Q Do you know what vpro.su is?
A I know it was a carding forum or a dumps shop. Regardless, it was carding related.
Q And what username did the user of the defendant's computer input when he logged on?
A "2Pac."

Q Scrolling down the page, what about Record Index Number 8, what website did the user log on to?
A Omerta.cc.
Q And what did the user log in as?
A "2Pac."
Q And Record 9, what was the website here?
A Vor.cc.
Q Do you know what that website related to?
A Again, it was a carding forum or dumps shop. I can't remember which one, but it was carding related.
Q What username did he use?
A "2Pac."
Q Let's scroll up here to this one.
For Record Index Number 10, what is the website that he logged on to?
A BTC-e.com.
Q And what is the BTC-e website?
A It's a Bitcoin exchange, where a user could go to buy and sell Bitcoin.
Q And how, if at all, was Bitcoin used in the 2Pac website?
A It was a form of payment that was accepted there.
Q And is that an e-mail that we just spoke about a minute ago?
A It is.
Q And then what was the password that was used on the

Bitcoin site?
A "Smaus123," capital "S."
Q Let's look at Record Index Number 11.
What website was visited here on the defendant's computer?
A Crimes.ws.
Q And what username?
A "2Pac."
Q And the next one here?
A The site inFrauD.su.
Q And the login?
A "2Pac."
Q Okay. Let's move on to a different topic now.
Did you ask Special Agent Mills to look for chats on the computer?
A Yes.
Q And for those people who might not know, can you just explain what a "chat" is?
A A chat can be obtained from an instant messaging service. It can be a realtime text conversation between individuals utilizing software. It's much like texting is on a cell phone, but it happens on a computer.
Q And were you and Agent Mills able to determine whether there were chat accounts that were set up on the laptop?
A Yes.
Q And is Exhibit 13.39 a copy showing the names of those

accounts that were associated with this laptop?
A Those are some of them, yes.
Q And is this an accurate replication of those?
A Yes.
MR. WILKINSON: The government offers 13.39.
MS. SCANLAN: No objection.
THE COURT: They're admitted.
(Exhibit 13.39 was admitted)
BY MR. WILKINSON
Q So what were the two usernames, or chat names, listed here?
A "Jaba2Pac.name" and "trackios."
Q Is Exhibit 13.32 one of the chats that Special Agent Mills retrieved from the computer?
A Yes.
Q And is this an accurate replication of it?
A Yes.
MR. WILKINSON: Government offers 13.32.
THE COURT: Any objection?
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 13.32 was admitted)
BY MR. WILKINSON
Q How many people are involved in this chat?
A Two.

Q Okay. And can you tell which one of them was the owner of the laptop?
A Yes.
Q And which one is it?
A The top one, trackios.
Q Okay. And how does trackios introduce himself in the first line of the text, right above "chat"?
A It says, "Hello. It's owner of 2Pac.cc."
Q And what does the other party to the chat say?
A Says, "Hello," and then says he has some dumps from the USA.
Q And does 2Pac -- or trackios make an offer to him?
A Yes. He asked if he wants to sell them through his shop.
Q And then what's the following discussion about a "valid rate"?
A They go on to talk about the validity rate, on how many of the numbers will be good to be posted on the site.
Q And as we look further down, there's an indication about, "My minimum is 2K now."
Do you know what that's referring to?
A Yes. My minimum is 2,000 pieces, or 2,000 cards.
Q What does that mean?
A Dumps, track information.
Q And then is there a discussion down below about how prices are set?

A Yes.
Q And how are prices set?
A Trackios indicates that others can set the price, but then they split it 50/50.
Q Was this the only chat that you found on the laptop that talked about buying and selling dumps?
A No.
Q How would you describe, generally, the nature of the chat conversations that you saw on the computer?
A Almost all of them are related to carding.
Q What is Exhibit 13.25?
A It's a copy of a chat from Miranda. It's a different instant messaging service program, which was installed on the laptop.
Q Is this an accurate representation of the chat taken from the laptop?
A Yes.

MR. WILKINSON: Government offers 13.25.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.25 was admitted)

BY MR. WILKINSON
Q Okay. Who are -- what are the names of the parties to this chat?
A "Director" and "Marysnow."

Q And which one is the owner of the laptop?
A Director.
Q And what does Director ask?
A Asks if an ad, or banner, can be placed on Mary Snow's shop, and then indicates he's selling dumps.
Q And what does Marysnow say?
A Talks about the monthly charges that would be required.
Q And remind us, did you see a banner ad on the defendant's laptop?
A Yes, both on the desktop and within that p.rar compressed file.
Q Now, scrolling to the bottom, does the user of Mr. Seleznev's laptop identify what -- where his banner is, where the banner ad is?
A There is mention of a forum on cardingforum.org.
Q Okay. And then where does -- well, if you look at the three highlighted lines in the middle of the page, what's he indicating here?
A "Look here. Here's my banner for the 2Pac.cc shop."
Q And we'll look at one more.
Is Exhibit 13.37 another chat taken from the laptop?
A Yes.
Q Accurate replication of the data on the laptop?
A Yes.
MR. WILKINSON: The government offers 13.37.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 13.37 was admitted)

BY MR. WILKINSON

Q How does the user of the laptop introduce himself in this chat?

A "Hello, it's 2Pac."

Q And does he make an offer to the person he's speaking with?

A Yes. He asks if the person wants to sell dumps in his shop.

THE COURT: Counsel, let's take a stretch break before you go to another exhibit.

Please be seated.

BY MR. WILKINSON

Q Okay. Agent Fischlin, I think to move things along a little bit, I'm going to ask you to review a number of exhibits. And then I'm going to ask you, at the end, whether they're all chats that were copied, and whether they're accurate representations of what was on the laptop.

A Okay.

Q So do you have the binder there that starts with Exhibit 13.21?

A No.

MR. WILKINSON: Okay. Ms. Ericksen, could you pass

him that binder, please?
BY MR. WILKINSON
Q And if you'd just review it, and tell me once you've looked at it, and we'll go on to the next one.
A All right. I've seen that one.
Q All right. 13.22?
A Okay.
Q 13.23?
A Yep.
Q 13.24?
A Okay.
Q 13.26?
A Okay.
Q 13.27?
A Okay.
Q 13.28?
A Okay.
Q And 13.29?
A Okay.
Q And are all of those accurate representations of chats that were retrieved from the laptop?
A Yes.
MR. WILKINSON: So the government would offer 13.21, 13.22, 13.23, 13.26 --
THE COURT: You skipped .24, Counsel.

MR. WILKINSON: Thank you, Your Honor. 13.24, 13.26, 13.27, 13.28, and 13.29.

MS. SCANLAN: No objection.

THE COURT: They're all admitted.

(Exhibits 13.21, 13.22, 13.23, 13.24, 13.26, 13.27, 13.28, and 13.29 were admitted)

BY MR. WILKINSON

Q And then one other item from the laptop, we looked at the document that you characterized as a passport -- as a password list; do you remember that?

A Yes.

Q Were there just one of those files, or were there several of them?

A There were several.

Q Okay. And I'm putting up 13.12A.

Is that another one of the password lists that was taken from the computer?

A Yes.

Q Is that an accurate replication of it?

A Yes.

MR. WILKINSON: Government offers 13.12A.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 13.12A was admitted)

////

BY MR. WILKINSON

Q Okay. I'd like to move on now to another topic.

In addition to the laptop, did you also examine an iPhone that was seized from the defendant?

A Yes.

Q Okay. And can you tell us, is examining an iPhone, or a phone, different forensically from investigating a computer?

A It is.

Q And in what ways?

A Well, with traditional forensics with a computer, you remove the hard drive from a computer, attach it to a write blocker, and then acquire an image to be examined later. Cell phones, how they're constructed, the storage medium is soldered within the device. You can't really remove it. As a result, the device will be started. It will be connected to, in this case, a Cellebrite universal forensic extraction device, which is designed to extract data from the cell phone. So it's simply different, is that you can't remove the storage medium to attach it to a write blocker and acquire that image.

Q So you mentioned the Cellebrite process for acquiring the image.

Is that a widely accepted software, or process, in the field?

A Yes. It's used by private industry and the federal government, law enforcement, military. It's a widely used

product.
Q Do you have Exhibit 12.8A up there?
MR. WILKINSON: Or Ms. Ericksen, do you have that?
BY MR. WILKINSON
Q Do you recognize Exhibit 12.8A?
A Yes.
Q What is it?
A It is the cell phone recovered from the defendant when he was apprehended.
Q How do you know it's the same phone that was recovered from the defendant?
A His is inventoried. And the last four of the identifiers on the back, of 1871, the IMEI, I recognize that.
Q Did you do an examination of this cell phone?
A Yes.
Q And did you follow the Cellebrite procedure that you just described?
A I did.
Q Was it successful?
A Yes.
Q What sort of things were you able to recover as part of that process?
A We were able to recover photos, able to recover chats via a variety of different services, recover a large amount of data from the phone.

Q Did you look for items of dominion and control on the phone?
A Yes.
Q And remind us what items of dominion and control are.
A Items that would show who owned or possessed the device.
Q And did you find any?
A Yes.
Q Okay. And can you give us an example of what you found?
A Yes, a variety of photographs of the subject, on the phone.
Q And by "the subject," you mean Mr. Seleznev?
A Yes, the defendant.
Q Is Exhibit 14.4 one of the photographs that was on the phone?
A Yes.
Q Is this an accurate replication of it?
A It is.

MR. WILKINSON: The government offers 14.4.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 14.4 was admitted)

BY MR. WILKINSON
Q And what are we looking at here?
A It's a digital photograph of an international passport. It's the same one that was recovered from the defendant when he

was apprehended.
Q When you look at a photographic imagine taken from a cell phone, does it provide you with information about where the photograph was taken?
A It can, depending on the settings and the type of phone, yes.
Q And in this case, could you tell where this photograph was taken?
A Yes.
Q Where was it taken?
A Bali, Indonesia.
Q Is Exhibit 14.3 two more items, photographs, that were taken on the phone?
A Yes.
Q Are they accurate replications of them?
A Yes.

MR. WILKINSON: The government offers 14.3.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 14.3 was admitted)

BY MR. WILKINSON
Q What do we have in the first image here?
A It's a digital photograph. In this case, it's a self-portrait, or "selfie," of the defendant. In particular,

the -- it's an Apple iPhone in the picture, and it appears to be the same color as the cell phone that was recovered from the defendant when he was apprehended in the Maldives.

Q What about the second page of the exhibit?

A Another digital photograph, selfie, of the defendant.

Q And what did seeing these pictures, combined with the passport, tell you as far as dominion and control evidence?

A That the defendant appeared to be the owner of the device.

Q Is Exhibit 14.15 another collection of photographs found on the phone?

A Yes.

Q Are they accurate representations of those photographs?

A Yes.

MR. WILKINSON: Government offers 14.15.

THE COURT: Any objection?

MS. SCANLAN: Your Honor, if I may have just one second?

THE COURT: You may.

MS. SCANLAN: Your Honor, may we have a sidebar regarding this exhibit?

THE COURT: Okay. Members of the jury, you can stand up and stretch.

(The following proceedings were heard at sidebar)

THE COURT: 14.15 starts with this photograph.

MR. WILKINSON: And I'd note that we've actually

removed the first four pages of that, and they must not have been removed from your binder. So that's removed, that's removed.

THE COURT: So when you're saying "that," it's from .001 through .004?

MR. WILKINSON: Correct. And they've been renumbered on the official exhibits, but this is where it starts.

THE COURT: Okay. And when you say "this," you're referring to 14.15?

MR. WILKINSON: 14.15.001 on the actual court exhibit.

THE COURT: Okay.

MS. SCANLAN: So I'm just not sure. This is 14.15, and 14.15.002, .003, I'm not sure what the relevance is of these pictures.

MR. WILKINSON: The pictures are offered as evidence of unexplained wealth.

MR. BROWNE: How do you know if it's unexplained if you don't know if he was employed?

MR. WILKINSON: Well, there's no evidence or reason to believe that the defendant had any legitimate source of wealth. And the Ninth Circuit case law says that as long as the evidence could support the inference that it was wealth derived from a fraud, that it's admissible as unexplained wealth.

MS. SCANLAN: So -- and I should be more specific. I can see that as to Page 4 --

THE COURT: Okay.

MS. SCANLAN: And 6, 7, and 8. I don't appear to have Page 5. Yeah, we don't have Page 5. This was the substitute exhibit that was received. I don't have Page 5.

But just to finish, as to Page 1, 2, and 3, we -- I haven't heard anything about how these are even allegedly the defendant's vehicles, at this point. So what does this have to do with unexplained wealth?

MR. WILKINSON: Well, the defendant's in the photograph, and the vehicle -- frankly, I would be happy offering just 1 and 4. We don't necessarily need those.

MS. SCANLAN: I don't -- I still don't understand how this picture shows that -- the objection is that I don't think this picture shows the defendant has unexplained wealth. It shows him standing by a vehicle. That's different.

MR. WILKINSON: It shows him standing by a very expensive vehicle.

MR. BROWNE: That's not that expensive.

THE COURT: We won't get into that, Counsel.

Counsel, the Court's going to let you put the ones in that have reference to money. You'll have to establish more of a direct connection to the defendant, other than standing next to a car. Anybody could take a picture --

MR. WILKINSON: Your Honor, I would say this is also admissible as evidence of dominion and control, since it has a picture of the defendant.

MS. SCANLAN: This is duplicative of all the other pictures of him that are on the phone.

THE COURT: The objection is sustained as to the pictures of the car. The money comes in.

I want you to make a record of the ones that show the pictures of the money, because I'm not sure if it's clear now on -- as far as the exhibits that are trial exhibits. Because it's inconsistent with what I have, and it looks like it's different from what defense counsel has.

MS. SCANLAN: The only --

MR. BROWNE: There's one missing.

MS. SCANLAN: If I may, we don't have a copy of Page 5, so if I could see that before we --

MR. WILKINSON: Okay. I'll pull it up.

MR. BROWNE: Just one comment about what is marked 14.15.04, there's no evidence that this is his car, or anything. There's money.

THE COURT: It's on his cell phone.

MR. BROWNE: Okay.

THE COURT: That's the connection. The relevance threshold, Counsel, is pretty low. So with that, the objection is overruled as to that basis. The objection is otherwise

allowed, and will be sustained as to the vehicles.

But Counsel, as far as the money, clarify the record, and they're admissible. And counsel can make a record as far as what she's agreeing to and what she's objecting to.

MS. SCANLAN: And then so 14.15; 14.15, Page 2; and 14.15, Page 3, are excluded?

THE COURT: That's correct.

MS. SCANLAN: And the government is going to show us Page 5?

MR. WILKINSON: Yes.

THE COURT: Okay. All right.

(End of proceedings heard at sidebar)

THE COURT: Okay, Counsel. Please proceed.

MR. WILKINSON: I'm calling up 14.15.005. At this point, the government will offer 14.15.004, 14.15.005. I think we'll just offer those two.

THE COURT: Counsel, have you seen .005 now?

MS. SCANLAN: Yes, Your Honor. We have no objection to 14.15.004 and 14.15.005.

THE COURT: Those are admitted.

(Exhibits 14.15.004 and 14.15.005 were admitted)

BY MR. WILKINSON

Q What is Exhibit 14.15, Page 4?

A It's a digital photograph recovered from the iPhone. In particular, it shows a large amount of foreign currency in the

backseat of a vehicle.
Q And going to the fifth page of the exhibit, is that another of the pictures on the phone?
A It is.
Q And what do we see here?
A What appears to be a pretty substantial amount of foreign currency, and another individual on the photograph.
Q Is that an individual who's shown up in other pictures on the defendant's phone and computer?
A Yes.
Q And were they sometimes in the pictures together?
A Yes.
Q Specifically, I'll call up what's been previously admitted as 13.3.
Do you see the defendant in this picture?
A Yes. He's in the middle.
Q And do you see the man who in Exhibit 14.15 was holding -- with the large stacks of cash?
A Yes. He's to the left.
Q Do you recognize Exhibit 14.5?
A Yes.
Q What is it?
A A digital photograph recovered from the phone.
Q Is this an accurate representation of it?
A Yes.

MR. WILKINSON: The government offers 14.5.

MS. SCANLAN: I'm sorry. If I may have a moment? I can't really see that. I'm going to find the paper copy.

MR. WILKINSON: I can blow it up too.

MS. SCANLAN: May I ask a question of Mr. Wilkinson, quickly?

THE COURT: You may.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Agent Fischlin, are you looking at 14.5?

A Yes.

Q How is this -- what are we -- not the contents of it, but what are we looking at in terms of this image? How did you get this image?

A It's a digital photograph which was recovered from the iPhone.

Q This is -- this right here is a photograph that was on the phone?

A Correct.

Q So it's not a photograph that you took of a screen?

A No.

MS. SCANLAN: No objection.

THE COURT: 14.5 is admitted.

(Exhibit 14.5 was admitted)

DIRECT EXAMINATION

BY MR. WILKINSON

Q So you just said this was a photograph.

What is it a photograph of?

A Of a chat between 2Pac and CapitalZOne.

Q And is it in English or a different language?

A A different language.

Q And can you tell, from looking at the screen, whose side of the chat was being photographed? In other words, which side of the computer are we looking at?

A It appeared to be the 2Pac user.

Q And how can you tell that?

A If you look at near the bottom, you can see that CapitalZOne is typing a message, and the person -- in the photograph, you see this person is waiting for that text to appear. So it appeared that 2Pac was the actual person behind this computer.

Q Did you notice anything about the tabs in the lower right-hand side of the computer?

A Yes.

Q What did you notice?

A Near the bottom, one of the minimized tabs, in particular, it had the letters lower case "n," capital "C," lower case "u." And then after that, it stopped. But it appeared to be short

for the nickname "seek," or "nCuX." The capitalization of that alias would have been identical.

Q It's a little hard to see here, but is that where my arrow is pointing?

A It is.

Q 14.5A, the English translation of that chat?

A Yes.

Q Okay. And what, generally, was the chat about?

A Well, there was a reference to Try2Check, or the checker service Try2Check.me. And then later, there was a discussion about WebMoney and some form of payment.

Q What is Exhibit 14.1?

A That is a screenshot of a user screen from the iPhone.

Q And is that what it looked like on the actual iPhone itself?

A Correct.

Q And this is an accurate representation of it?

A It is.

MR. WILKINSON: The government offers 14.1.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 14.1 was admitted)

BY MR. WILKINSON

Q So what are we looking at here?

A Settings information for the phone, in particular for

iCloud.
Q And do the settings include what e-mail account was set up to operate with the phone?
A Yes.
Q And what e-mail account was that?
A Romariogro1@mail.ru.
Q And I'm scrolling down to the third page.
What are we looking at now?
A The settings information, in particular for FaceTime on the device. The two checked e-mails there are the ways that you could contact the individual on this phone via FaceTime.
Q And what are the two ways that you could contact them?
A Roman.seleznev@icloud and then romariogro1@mail.ru.
Q Do you recognize Exhibit 14.10?
A Yes.
Q What is it?
A A screenshot of an e-mail from the iPhone.
Q And is it a collection of e-mails?
A Yes.
Q And is it an accurate copy of all the e-mails that you found on the phone?
A Yes.
Q Not all, but some of those e-mails?
A Yes.
MR. WILKINSON: The government offers 14.10.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 14.10 was admitted)

BY MR. WILKINSON

Q Okay. Are we looking at the Russian version of it?

A We are.

Q And what organization are the e-mails to and from?

A From BTC-e.

Q And what's that?

A That's a Bitcoin exchange, where users can buy and sell Bitcoin.

Q And we're jumping now to the English translation of that, which is 14.10A.

Did that page indicate what the login was for the account?

A Yes.

Q And what was it?

A "Smaus."

Q And going to the second page of this collection of e-mails, is this a different e-mail?

A It is.

Q And also from the Bitcoin exchange?

A Yes.

Q And what's this one saying?

A "Dear smaus, we have received a request to transfer out US dollars 21,000 to wallet." And then it lists a Perfect Money

account.
Q Going to the fifth page, another e-mail?
A Yes.
Q And what does this one say?
A "Dear smaus, we have received a request to transfer out US dollars 31,000 to wallet." And it's a Perfect Money account.
Q Going to Page 11 of the exhibit, what do we have?
A Another e-mail from BTC-e. It says, "Dear smaus, we have received a request to create a BTC-e code in the sum of US dollars 10,000."
Q Do you recognize Exhibit 14.11?
A Yes. It's a screenshot of another e-mail that was recovered from the phone.
Q Is it an accurate copy of the e-mail?
A Yes.
MR. WILKINSON: The government offers 14.11.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 14.11 was admitted)
BY MR. WILKINSON
Q Who is the e-mail from?
A I cannot make it out on this photo.
Q Can you read the text at the top?
A Sure. "On Wednesday, June 18," gives a time, "2014, RU-CENTER received a request from IP address 212.17.164.128

[sic] for the administrative password to enter the 'manage your account' section under the agreement," and then it gives an agreement number.

Q And what was the password associated with the account?

A "Ochko123."

Q Okay. Let's move on to another topic.

As case agent on this case, did you do any investigation into an intrusion at a local business called Red Pepper Pizza?

A I did.

Q And when was this?

A That was in August of 2014.

Q And how did that compare in time to the defendant's arrest?

A It was after.

Q And why did you -- what caused you to go contact Red Pepper Pizza?

A Well, during Special Agent Mills' examination of the laptop recovered from the defendant, he'd found, early on in that exam, dump files with credit card information that appeared to be named after states. One of them, in particular, 1000 Washington, he notified me, when he found that file. And I asked for the contents of that file so I could reach out to financial institutions to see if there was a common point of compromise.

So within that file, there was approximately 65 American

Express account numbers. I had a good cyber investigator contact at American Express, so I sent her those account numbers and asked her to let me know, did all these customers, account holders, go to someplace in common, which could have been a point of compromise. She --

MS. SCANLAN: Objection.

THE COURT: If it's going for a response from someone else, that objection is sustained.

BY MR. WILKINSON

Q What did you do in response to the conversation with the person from American Express?

A I responded to Red Pepper Pizzeria. I spoke to the owners, and ended up getting authorization to examine their point-of-sale systems, which had actually been taken out of service several months prior. They were sitting in the garage of the owners. They provided me authorization to search those systems, and I subsequently did so.

Q Okay. Did you find evidence of an intrusion on those systems?

A I did.

Q And did you create an exhibit for court that shows some of the computer artifacts that you found on the system?

A Yes. It shows some of that data.

Q Do you recognize Exhibit 1.10?

A I do.

Q And is that the exhibit you created?
A Yes.
Q Is that copies of actual computer artifacts that you copied onto that page?
A Yes.
MR. WILKINSON: The government offers 1.10.
MS. SCANLAN: Is it just one page?
MR. WILKINSON: It's just one page.
MS. SCANLAN: May I inquire?
THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN
Q This is -- I think you just said this is a copy of something from a computer; right?
A Yes.
Q From what computer?
A So these are -- these were obtained from Red Pepper's point-of-sale systems. And these are screenshots taken with forensic software during the exam of their systems.
Q So each of these blue boxes is a separate screenshot?
A Yes.
Q Did you take the screenshots?
A I did.
MS. SCANLAN: No objection.
THE COURT: 1.10 is admitted.

(Exhibit 1.10 was admitted)

DIRECT EXAMINATION

BY MR. WILKINSON

Q So can you, using this exhibit, point out what the significant forensic artifacts were, relative to this intrusion?

A These are some of the artifacts of interest. Up top, the very first screen capture, fDenyTSConnections, that shows the setting in the registry for remote desktop. In particular, this indicates that remote desktop was enabled. It was on for the system.

Q Let me ask you a question about that. We heard testimony earlier from Detective Dunn about Port 3389.

Was Port 3389 open on this computer?

A It was. That's what this setting would show.

Q And please continue with the significant artifacts here.

A The next screenshot shows the usernames and passwords for the system. In particular, there was an administrator, and the password was "rev12230." And there was a second account on that system, and the username was "user," and the password was "user."

Q And then what about this next set of items?

A It's a screenshot of some of the software installed on the system at the time of compromise, on or about that time. It shows that PuTTY was installed on the system. PuTTY is free

software, open source. And what it does, it allows for SSH, or Secure Shell, Intelenet connections to assist them. So you can remotely connect to a system or transfer files between computers with this software.

Q Let me just put that up next to Exhibit 13 -- what's previously been introduced as Exhibit 13.9, and specifically the 17th page of it.

Is this a list of some of the dump files found on the defendant's computer?

A Yes.

Q And what are Items 121 and 122 named?

A Putty.txt and putty2.txt.

Q Okay. So please continue with any other significant items you saw here.

A The next screenshot shows installation of malware. In particular, this was Perfect Keylogger.

Q What is Perfect Keylogger?

A It is software designed for surveillance. So it's a keylogger. It can capture a user's keystrokes. It can be set to capture screenshots of the computer, and can be designed to or set to log all data that an application is performing on a computer.

Q Was this software that the user had installed, that the owner of Red Pepper Pizza had installed?

A No.

MS. SCANLAN: Objection.

THE COURT: Do you still wish to maintain an objection, Counsel?

MS. SCANLAN: Well, I was going to object that the answer is based on hearsay.

THE COURT: Let's clarify, Counsel.

What's the source of the information?

BY MR. WILKINSON

Q Do you know whether this was user-installed software?

A No. It doesn't appear to be.

Q Is your knowledge of that fact based on conversations you had with the user, or is it based on your examination of the the computer?

A Both.

THE COURT: Objection is overruled.

BY MR. WILKINSON

Q And continuing down below, what do we have here in this last set of items?

A So that is a user program to decode the Perfect Keylogger configuration file. And this shows the results. The top line, after "C:" and that string of characters, that shows where the log files for Perfect Keylogger would be stored on that system. The next line shows the license key name. The next line shows the license key. And the final line, of "2pacsakur," that shows that was the password to access Perfect Keylogger on the

system, to actually control it.
Q And you said that there's this path where these log files would be stored.
Did you find log files?
A Yes, on each point-of-sale terminal.
Q And what was in the log files?
A Within those Perfect Keylogger log files was track data.
Q And by "track data" you mean?
A Credit card track data.
Q Did you create a video to show how the Perfect Keylogger software worked?
A I did.
Q Is Exhibit 1.10A an accurate copy of that video?
A It is.
Q And is it a copy that you made yourself?
A It is. It is actually a virtual machine. It's a copy of the system. It's a software copy so we can see it, much like the user of the point-of-sale terminal would if they were to boot it up.
MR. WILKINSON: The government offers 1.10A.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 1.10A was admitted)
BY MR. WILKINSON
Q Okay. So what are we looking at right now?

A So this would be the desktop of that point-of-sale terminal, in a virtual machine. The only thing I created here was the text file you're looking at. That was kind of -- so you could read what was happening.
Q And that -- by "text file," you mean this box here?
A Yes. That's the only thing.
Q And what did you type in the box? Why don't you just read it out loud.
A Sure. "Notice that Perfect Keylogger is hidden, at first. There's no system tray icon for it." So in the bottom right, there's no icon for that program. You'd have no idea that it is running on the system.
Q And then what did you write next?
A "Once the correct key combo is entered, Windows key plus '0' in this case, the user is prompted for a password. '2pacsakur' is entered."
Q So this is what Red Pepper Pizza's computer would have looked like?
A Yes.
Q And is there any way for them to tell, when operating their software, that this software was installed on there?
A No. It was in hidden mode. You would not be able to tell, as a user.
Q Okay. In simple terms, how do you get it out of hidden mode? How do you make that software start working?

A You have to know the correct key combo, which was Windows key plus "0," and then you'd be prompted for a password.
Q So I'm going to play it on the video now. And you can just let us know what's happening -- actually, why don't you tell us, first.
What are you going to do?
A Sure. So I'll end up pressing the Windows key and "0" at the same time. You'll suddenly see a prompt pop up, asking for a password. I'll then enter the password, "2pacsakur," and then I'll be granted access to the control panel for Perfect Keylogger. With that control panel, you'd have complete control over that program.
Q I'll push play now. And tell us when you push that hot key that makes the software appear.
(Video recording playing)
A I will here in a moment.
In the bottom right, I was showing that there's no icon for it. I just hit Windows key plus "0," and a prompt pops up asking for a password.
Q So this box pops up when you press the right keys?
A Yes.
Q Now, what password are you entering?
A "2pacsakur." At which time, now on the bottom right there is an icon for Perfect Keylogger. I'll subsequently click on it and have control of the program. I'll kind of show some of

the settings that were enabled on it. That's what I'll do subsequently; show what version of Perfect Keylogger was installed.

Q Now, with Port 3389 open, are these all things that could have been done remotely, from outside the restaurant?

A Yes. These are some of the settings for Perfect Keylogger on the system. You can see that "show" or "hide it." You'd use Windows key plus "0," or zero.

Here's some of the logging options set for it. So it's set to capture chats, button clicks, passwords, enable clipboard logging, monitor online activity. That's where the logs would be stored. There's the setting for it. Screenshots were not enabled, so it was not taking screenshots. It was not set to automatically e-mail out the log file. And it wasn't configured to FTP, or transfer out log file in that protocol either.

Q How would the credit cards have to be gathered by the off-site person?

A I believe that a user -- someone would have to come back into the system to obtain those log files.

And that's where you can change the password, if you wish. That's the last box.

(End of video)

Q Okay. Thank you.

Did you find any of these -- I think you've been referring

to them as "log file"?
A Yes.
Q And did they actually contain credit card data?
A They did.
Q Is Exhibit 1.11 a collection of some of that data from Red Pepper Pizza?
A Yes, that's some of it.
Q Is it an accurate copy?
A Yes.
MR. WILKINSON: The government offers 1.11.
MS. SCANLAN: No objection.
THE COURT: Admitted.
(Exhibit 1.11 was admitted)
BY MR. WILKINSON
Q So what are these lines of data here?
A It's Track 1 information. So it would be credit card data, cardholder name, and then discretionary data.
Q And what is the cardholder name in the first line?
A Ruth Gebhard.
Q And is that the person that's identified in the charges in this case as "R" -- in one of the charges in this case as "RG"?
A Yes.
Q Is that the credit card number that's referenced in the charges relating to RG?
A Yes.

Q And have you met Ms. Gebhard?
A I have.
Q And how did you meet her?
A I interviewed her after locating her account number on the system.
Q Did you find this credit card data, these credit card numbers, in the collection of credit card files that were found on the defendant's computer?
A Yes. Out of the credit card numbers found on Red Pepper, about 235 of them, approximately, that are found on Red Pepper's systems, in those log files, were also found on the defendant's laptop.
THE COURT: Counsel, it's 2:45. Is this a convenient time to break?
MR. WILKINSON: Okay. Could I have one minute, Your Honor, just to finish up one little thing?
THE COURT: Certainly.
MR. WILKINSON: Thank you.
BY MR. WILKINSON
Q Okay. We're going to what's previously been admitted as Exhibit 13.11, as some of the dump files located on the defendant's computer.
And do you see Ms. Gebhard's name and computer -- excuse me -- credit card number on here?
A I do, right under that highlighted area.

Q So sitting here on the left, just to sum up, where was this data found?
A On the left, that was on one of the Red Pepper point-of-sale systems, in particular one of the Perfect Keylogger log files.
Q And the same data on the right was found?
A On the defendant's laptop, within one of the dump files named after the state.
MR. WILKINSON: Thank you, Your Honor. This is a good place to break.
THE COURT: Members of the jury, we'll take our afternoon break at this time.
(Jury exits the courtroom)
THE COURT: Counsel for the government, approximately how much more time do you have?
MR. WILKINSON: Ten minutes.
THE COURT: All right. And anything else to take up, by the government?
MR. WILKINSON: No, Your Honor.
THE COURT: By the defense?
MS. SCANLAN: No, Your Honor.
THE COURT: We'll be in recess.
(Recess)
(Jury enters the courtroom)
THE COURT: Counsel, you may continue your direct

examination.

MR. WILKINSON: Thank you, Your Honor.

BY MR. WILKINSON

Q Inspector Fischlin, when we left off, we were talking about the stolen -- or the credit card data that was saved in log files on the Red Pepper Pizza point-of-sale system.

A Yes.

Q Did you do anything with those credit card numbers after you collected them?

A Yes. I gave them to the Secret Service CRS, or Criminal Research Specialist, within the Seattle Field Office, Megan Wood, so she could then reach out to the issuers, or financial institutions, to determine if there was any loss on those accounts.

Q Did you do that with all the card numbers from Red Pepper?

A Yes.

Q And did you go through that same process with any other card numbers that you collected in this case?

A Yes; all the card numbers recovered from the defendant's laptop, as well as another server.

Q And what was that other server that you collected credit cards from?

A 2Pac.cc.

Q And so what was that server used for?

A For hosting the site. And via international process, a

copy of the forensic image of that server was obtained. Detective Dunn did the examination. He gave me the credit card numbers recovered from that server, and then I gave them to our Criminal Research Specialist to follow up on for potential fraud on the accounts.

Q You testified earlier that you were the case agent at the time of the defendant's arrest.

Did you continue to follow the 2Pac website after the arrest?

A I did.

Q And did you take screenshots to preserve things that were posted on the website?

A Yes.

Q And is Exhibit 10.3 an accurate copy of some of the screenshots of postings on that website?

A Yes.

MR. WILKINSON: Government offers 10.3.

MS. SCANLAN: I believe the defense already moved to admit this exhibit, Your Honor.

THE COURT: 10.3 has been admitted, Counsel.

MR. WILKINSON: That's right. Thank you.

BY MR. WILKINSON

Q And I'd like to direct your attention to the third page of the exhibit.

What is the date of the entry I've blown up here?

A July 8, 2014.
Q And we might be used to looking at that and saying "August 8" [sic].
Why do you say "July 8"?
A Well, we can see within the text of the body how it's referencing, "Till 16th July there will be a short vacation." That helped me with the date, as well, since that would have been shortly after this time frame, while a vacation was taking place.
Q Is that the international convention for writing dates?
A It is.
Q And how did the date of this posting compare with the date of the defendant's arrest?
A It was a few days after.
Q And what does the posting say?
A "Till 16th July, there will be short vacation. During this time, there will be less updates than usually, and longer refund/support respond time."
Q Did the website continue to be up and operating through July?
A Yes.
Q And did that surprise you, even though the defendant was in custody?
A No.
Q Why not?

A Because we believed there would be co-conspirators assisting, operating the site with him.
Q And I'd like to direct your attention to the first entry on the exhibit.
What's the date there?
A August 8, 2014.
Q So about how long after the defendant's arrest is this posting?
A Just over a month.
Q And what does the posting say?
A "Dear customers, we apologize for the inconvenience that you are experience now by the fact that there are no updates, and checker doesn't work. This is due to the fact that our boss had an car accident, and he is in hospital. We will solve all problems as soon as possible. Support always available. Thank you for your understanding."
Q Now, at this point in time, had the U.S. government revealed publicly that it believed that the defendant was the identity behind 2Pac?
A No.
Q And at some point, was that publicly revealed?
A Yes, about a week, week and a half after that.
Q How was it revealed?
A During a hearing here in the courthouse.
Q And was it stated by the government, publicly?

A It was.
Q Did you go back and check the website after that to see if it was still operating?
A I did. That hearing concluded around 3:00 p.m. And around approximately 9:00 p.m. that evening, I went to the site, and it was down. It was no longer available on the internet.
Q Was the site put back up, at some point, after that?
A Yes. Sometime in September, approximately September 12, it came back up.
Q Okay. And again, did that come as a surprise to you?
A No.
Q And why was that?
A Again, we believe that co-conspirators were assisting with the operation of the site.
Q We touched on this earlier, but was the site then subsequently taken down after that?
A After September?
Q Yeah.
A Yes, it was.
Q And who was it taken down by?
A German authorities.
MR. WILKINSON: No further questions.
THE COURT: Cross examination?
////

CROSS EXAMINATION

BY MS. SCANLAN

Q Good afternoon.

A Good afternoon, ma'am.

Q Okay. Let's start back where we just ended, so 10.3.

You were testifying that there was information in Seattle, in a courtroom like this; right?

A Yes.

Q That the government thought 2Pac was Mr. Seleznev; right?

A Yes.

Q And then how many hours later?

A Approximately six hours later.

Q It went down.

A Correct.

Q But you don't have any evidence of communication from Mr. Seleznev with anyone else about that; correct?

A That's correct.

Q Between the time of Mr. Seleznev's arrest and when the site went down, there was quite a few things happening on the site; correct?

A There was still activity on the site. That's fair to say.

Q And that's what we're seeing in 10.3, if we can pull this up so you can see it?

MR. WILKINSON: Top half?

MS. SCANLAN: How about just the text. This works.

BY MS. SCANLAN
Q Yes. So, I mean, we're not talking about just little updates; right? So July 28 of 2014, there's a dump update; right?
A Yes.
Q July 31, update; right?
A Yes.
Q August 1, big update.
What is this? "I present you with another big dumps update from E-Dump."
A Yes.
Q And then the vacation thing happens kind of after all of that happens; right?
A Just after that post appeared, yes.
Q So Mr. Seleznev was arrested around July 4, July 5?
A Yes.
Q And there's all this activity after that, and then the vacation post was in early August?
A Yes.
Q Okay. So let's go back to the Red Pepper Pizzeria.
You indicated that there was something called "Perfect Keylogger," that you found installed on the point-of-sale systems for Red Pepper Pizzeria; right?
A Correct, all three.
Q All three point-of-sale terminals?

A Correct.
Q Did they have a back-of-the-house server?
A They did.
Q Did that have it on it?
A It didn't.
Q It didn't?
A No.
Q Just the point-of-sale terminals?
A Correct.
Q And the point-of-sale terminal is, like, where -- if you're standing here, and you work in a restaurant, where you're punching in orders and running credit cards; right?
A Correct.
Q And the back-of-the-house server is the thing that's traditionally in the office, the computer that's connected to the point-of-sale terminals?
A Correct.
Q And Perfect Keylogger is a commercially available software?
A That is right.
Q So it's not something that's particularly unique or within this kameo malware family?
A That's accurate.
Q And when you looked at the -- you looked at the antivirus logs for that point-of-sale system; right?

A I did.
Q What are antivirus logs, again?
A Show if a virus scan's been done on a system and if there's any finds.
Q And when you did that, there were variants of Alina; right?
A On the point-of-sale terminals, there was one other piece of potential malware on each of them. And then on the server there was a variety of malware that antivirus logs had hit on.
Q Some of them named "Alina" and "Dexter"?
A Correct.
Q And Alina and Dexter are not kameo; right?
A True.
Q Okay. The iPhone?
A Yes.
Q You received the iPhone. You noted that it was in airplane mode; right?
A Yes.
Q Why was that significant? Why did you note that?
A I noted it just to note the condition it was in when I took it as an actual examiner.
Q But do you know why, as an examiner, you would put the iPhone in airplane mode before you examined it?
A Sure. At that point, to ensure it was isolated from the network, prior to examining it.

Q From any network connectivity?
A Yes.
Q And why are you making sure that it's separate from that before you examine it?
A You want to ensure that at that point, when you're examining it, that -- potentially, if there's network connections, it could be remotely wiped, for example. You wouldn't want that to happen. Then you don't want any changes. You don't want incoming text messages, or anything like that, that's changing the state it was in when you received it. So you want to try and limit changes made to the device.
Q So ideally, you want the device to be in exactly the same state it was in when you seized it?
A No. As an examiner -- not necessarily. Because as an examiner, you can change some settings prior to actually examining it.
Q Okay. So what settings would you change before you examined it?
A That's a good example. Prior to examining it, I put the device, often, in the airplane mode. That's one of the things I often do, when I'm examining a mobile device, as an examiner.
Q Okay. That change doesn't change the files on the iPhone; right?
A No.
Q So that's a limited change that you make to control other

potential changes to this phone.
A Correct.
Q And so that's an iPhone, and that has potential cellular connectivity; right?
A It does.
Q And you know now that the Sony Vaio laptop tablet, with the screen up thing, that has potential connectivity, as well; right?
A I know that it had a SIM card, now, yes.
Q Okay. And a SIM card is a way that you have this potential connectivity; correct?
A Potentially, yes, can potentially connect to a cellular network.
Q So I want to talk about the laptop.
You've testified about the laptop as an exhibit, and you've been testifying for a while about the files you found on it, that Agent Mills gave you, et cetera; correct?
A Yes.
Q And you were also part of handling that exhibit when it was brought to Seattle from Agent Iacovetti?
A Yes.
Q So the laptop arrived on July 8 of 2014?
A Yes.
Q You picked up the laptop and Agent Iacovetti at the airport?

A I did.
Q And you guys went to your Secret Service office?
A Correct.
Q And that office is about three-fourths of one floor of an office building; is that right?
A Yeah.
Q And you took the laptop into a conference room?
A Yes.
Q You guys -- you laid it out on the table?
A Yes.
Q Do you know if there was a power adapter with it?
A There was, yes.
Q And I guess I should be more -- a power cord, something you can plug it into a wall with.
A Yes.
Q And so Agent Iacovetti had filled out these temporary evidence forms; right?
A Yes.
Q And those have make, model, serial number; correct?
A Yes.
Q And so when you guys laid it out on the table, you were going to put that information from the exhibit, or the laptop, onto a permanent evidence form; correct?
A Correct, and verify it.
Q And you did that; right?

A Yes.
Q So you took -- you looked at the laptop, and you put the serial number on the permanent evidence form?
A Yes.
Q And that was on July 8?
A Yes.
Q And then you took the laptop, and you put it in the main evidence vault; right?
A That day, yes.
Q And your office floor has two vaults; right?
A It does.
Q You've got the main evidence vault; correct?
A Yep.
Q And then the ECTF evidence vault.
A Correct.
Q And that's your task force vault.
A Yes, a temporary vault for electronic evidence.
Q So you put the laptop, on July 8, into the main vault; right?
A Yes.
Q Okay. Or did you do that, or did someone else do that?
A Our office manager, Elaine Rolf (phonetic), would have put it into the main vault.
Q And then the next day, you take it out of that vault; right?

A I did.
Q That's July 9?
A Yes.
Q And I'm sorry, what's the office manager's name again?
A Elaine Rolf.
Q Rolf?
A Yes.
Q Ms. Rolf took it out, but didn't sign it out; right?
A That's true.
Q And when we say "sign it out," we're talking about the evidence log sheets; correct?
A Correct. She didn't put a notation on the log sheet for the vault, but it was in the chain of custody.
Q Sure. But it's not on the log sheet; right?
A True.
Q And the log sheets say "sign in and out"; right?
A Yes.
Q So she takes it out of there.
Were you there for that?
A I don't know if I was there when she took it out. I did receive it. If I didn't get it at that point, I got it right after, because I remember I did walk it down.
Q And you walked it -- well, can't be that far; right?
A No.
Q So one vault to the other is approximately how far?

A Just a guesstimate --
Q Yeah.
A -- fifty yards.
Q Okay. So you walk it the fifty yards down to your vault; right?
A Yes.
Q And you -- this is July 9; right?
A That was, yeah.
Q You put it into your vault?
A Yes, the ECTF vault.
Q And was Agent Mills with you when you put it into the vault?
A He was.
Q And, now, is this when you guys went and looked for the serial number again?
A We did.
Q So just so I understand, Agent Iacovetti took the serial number when he seized it; right?
A Yes.
Q You verified that, on the 8th.
A I did.
Q And then on the 9th, when you and Agent Mills are in the vault, you decided to identify the serial number again?
A I did. Very redundant, but everything that goes in that ECTF vault is inventoried yet again; so, yes.

Q But not everything; right? Because Agent Mills never signed in and out of the vault that day.
A Well, it's still inventoried into that vault, so we still went through that procedure.
Q How about the people, though, who came in and out, they didn't all write on the log sheet; right?
A That's correct.
Q So you -- you wrote that you went in the vault.
A Yes.
Q And you wrote that you left the vault, like, eight hours later or something.
A I noted when the vault was secured for the day, yes.
Q Did you note when you went in and out of the vault?
A No.
Q Did you note when Agent Mills went in and out of the vault?
A No.
Q Aren't you supposed to put on the sheet whenever anyone goes in and out?
A According to the form, yes. However, that was not office practice.
Q Okay. So the Secret Service creates these forms; right?
A Yes.
Q And those forms, that are created by that federal agency, say that that's what you're supposed to do; right?

A That's what the form says.
Q That's what the form says; but you and Agent Mills didn't do that.
A We didn't -- that wasn't office practice.
Q Okay. What's the purpose of a vault?
A It's a place to secure evidence.
Q And you secure it by monitoring who goes in and out and who has access to it; right?
A Controlled access, yes.
Q So, now, this third check with the serial number, the laptop is in the vault; right?
A Yes.
Q You and Agent Mills are in there.
A Yes.
Q And then Agent Mills is the one handling the computer; correct?
A Correct.
Q And he is looking, ostensibly, for the serial number, and the screen comes on.
A Yes.
Q Now, let's back up one step.
Agent Iacovetti, had he told you that the screen turned on on the plane?
A He had.
Q So at that point, you knew that the computer had power.

A I knew that it had. I didn't know that it still had it.
Q Okay. You knew it had power in the conference room; right?
A No.
Q Oh, that's right. I'm sorry.
You knew that it had power on the plane, because he told you it turned on; right?
A Yes.
Q What happened -- and then he said he put a bottle cap over the power button; right?
A He did.
Q What happened to the bottle cap?
A I don't know. I remember us specifically talking about that bottle cap, but I cannot vividly remember it.
Q Okay. But it came in with all this evidence that you were, in some part, responsible for tracking; correct?
A Yes.
Q So you're in the vault, that day after the laptop comes in, and the screen comes up; correct?
A Yes.
Q And at this point, you had reason to be concerned that this computer might be encrypted; correct?
A Correct.
Q And when a computer is encrypted, if you want to image it, the idea is, you want to do a live image; right?

A You want to capture RAM, volatile data, yes.
Q And that RAM, volatile data, has to be collected when it's on.
A Yes.
Q If it turns off, and it's encrypted, you're not getting back in there; right?
A It's generally true, yes.
Q I think another way it's been referred to is, it becomes a brick. You can't get in it.
A Generally, yes.
Q So you're worried about encryption.
A Yes.
Q Even backing up to the conference room, Iacovetti tells you it's on. So did you plug it in?
A No. No. He told me that he'd seen it come to life on the plane, but not when we had it in the conference room, so I did not know it still had power, at that point.
Q Did you check?
A No.
Q Did you check to see if the light was flashing?
A No.
Q Okay. So it might have been on; right?
A It might have been in some sort of sleep state, yes.
Q Well, now we kind of know it was on in the conference room, right, because it turned on the next day in the vault?

A Yes. It had some form of power.
Q Okay. So when it's in the vault and you guys have the power cord, you didn't plug it in?
A I didn't.
Q So you left it in there, even though you're worried about encryption?
A Yes.
Q And then it stayed in there for the next 20 days?
A Approximately.
Q Okay. And at any time in that 20 days, since you were worried about encryption, did you go and try to plug it in?
A No.
Q Did you turn it off?
A No.
Q And you're aware that there were file changes to some of the files on that computer during that time period it was sitting there; right?
A Yes.
Q You indicated that you know now that that laptop tablet had cellular connectivity capabilities.
A We know it has a SIM card now, yes.
Q Is that some differentiation that I'm missing? I thought a SIM card meant that it had cellular connectivity capabilities.
A It means it can give a device the potential to connect to

a network.
Q So it has the potential to connect to a network; correct?
A Yes. If the SIM card's active, yes.
Q And there on the back of that -- we found this out a couple months ago; right? On the back of the laptop, there's an arrow, and it points to the SIM card.
A Yes.
Q If you had realized that had a SIM card in it, then you probably would have put it in a Faraday box; right?
A No.
Q So if you knew it had cellular capabilities, would you have brought it to your lab and put it in a Faraday box?
A If I knew that it had, like, an active potential connection, this was a laptop, not a mobile device, the only difference I would have done, in hindsight, 20/20, is potentially remove the SIM card. But with what we knew at the time, I wouldn't -- I don't think we did anything wrong. I think it was the right procedure.
Q Do you remember testifying in June?
A Yes.
Q I'm going to hand you a copy of that testimony; okay?
A Okay.
MS. SCANLAN: May I approach?
THE COURT: Yes.
THE CLERK: Defendant's Exhibit 112 is marked.

BY MS. SCANLAN
Q Inspector Fischlin, why don't you flip through that and just see if it looks like an accurate record of your testimony.
A I believe it is.
Q Can you turn to Page 44, please?
A Sure.
Q And actually, if you want to just start reviewing to yourself, silently, from the bottom of Page 43 through the first ten lines of Page 44.
A Okay.
Q Do you see that?
A Yep.
Q Okay. So the question is, if it has cellular capabilities, right, like a tablet, and you knew that, would you have put it in a Faraday box?
A Could you rephrase the question, or ask it again?
Q Yeah. So we're talking about a laptop --
A Yes.
Q -- has a cellular capability.
A Yes.
Q If you had known that that laptop/hybrid tablet, right, had this other capability, would you have put it into a Faraday box?
A With what we know now?
Q Okay. You've got a laptop tablet with cellular

connectivity capability; right?
A Yes.
Q Okay.
A To me, it's two different things, a laptop and a tablet.
Q Okay. In terms of their connectivity capability with a SIM card?
A Just their architecture. They're different devices. I treat them differently. That's how I've been trained.
Q So you're saying that if a tablet has a SIM card, you treat it different than a laptop with a SIM card?
A I'm saying that with a laptop, I had not seen one with a SIM card before this. I'd never even heard of a laptop containing a SIM card, before this one.
Q Right. And I'm not trying to say that you had heard of it. Right now, we're talking about devices that have this connectivity capability; okay?
A Yes.
Q You have acknowledged that this device, we know now, had that capability; right?
A Yes.
Q All I'm asking you, is, that if you had found the SIM card on the back of it, at that time, would you have done something to limit its connectivity abilities?
A In an abundance of caution, with what we know now, yes. And there's two options. One is to simply remove the SIM card.

That's a very easy option. The second is to put it into a shielded test enclosure. So either would complete that task.

Q Okay. And just to be clear, so when we talked about this before, in June, you said that you would have brought it into your lab, put it in a shielded test enclosure -- which is a Faraday box; correct?

A Yes.

Q Okay. We're done with the transcript for now.

A Okay.

Q Okay. I want to skip back to Red Pepper Pizza for a second; okay?

A Sure.

Q So you were talking about the Perfect Keylogger software; right?

A Yes.

Q And this is this commercially available software that you found on the Red Pepper system?

A Yes.

Q It didn't have coded into it an exfiltration site to send credit card numbers; right?

A Correct.

Q So whoever took the credit card numbers from Red Pepper Pizza had to go in and get them.

A Yes.

Q And there was no evidence of that exfiltration; correct?

A No, there wasn't. The security event logs, for example, were empty, so it's tough to tell from the logs what was occurring. And the other logs didn't go back to the time frame of the malware installation.

Q Okay. So we didn't actually -- we, you -- didn't actually see, within your examination, how the credit card numbers got out of Red Pepper Pizza to wherever they went; correct?

A Correct.

MS. SCANLAN: I have nothing further.

THE COURT: Redirect?

REDIRECT EXAMINATION

BY MR. WILKINSON

Q You just testified that there was no evidence of the credit card data on the Red Pepper system being exfiltrated out of the system; is that right?

A Correct. I don't know how it got out.

Q But where did you find the credit card numbers that were on that system?

A I found them both in the Perfect Keylogger log files, on the point-of-sale terminals from Red Pepper, as well as 235 of them, approximately, were found on the defendant's laptop.

Q Ms. Scanlan asked you about the nature of the malware, or software, that was found on the Red Pepper computer, and it not being part of the kameo family.

Do you remember those questions?

A Yes.
Q When did Detective Dunn -- in what year did he respond to the Schlotzky's and Broadway Grill, and those sites, where the kameo software was found?
A I believe it was 2010.
Q And in what year did you respond to the Red Pepper Pizzeria and find the Perfect Keylogger?
A 2014.
Q Do you use all the same software today that you used in 2010?
A No.

MR. WILKINSON: No further questions.

THE COURT: Re-cross?

RE-CROSS EXAMINATION

BY MS. SCANLAN

Q Just to be clear, so you said that you found credit card numbers on the laptop that we've been talking about.
A Yes.
Q That match the credit card numbers that were taken from Red Pepper Pizza.
A Yes.
Q But you have no idea how those credit card numbers got from Red Pepper Pizza to that laptop; correct?
A Correct.

MS. SCANLAN: I have nothing further.

THE COURT: Counsel for the government?

MR. WILKINSON: No further questions, Your Honor.

THE COURT: Any objection to this witness being excused?

MR. WILKINSON: No, Your Honor.

THE COURT: By the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you, sir. You're excused.

THE WITNESS: Thank you, Your Honor.

THE COURT: You may step down.

MR. WILKINSON: Your Honor, I think we're ready to break there for today, if that's acceptable.

THE COURT: Ladies and gentlemen of the jury, a surprise gift for you. We're going to break early today so you can go out and enjoy that 90-plus-degree weather early. We'll start again on Monday, at 9:00 a.m.

Now, I told you I'd give you updates so you know exactly where we stand today. Counsel for the government has given me their best projection, and they believe that they'll be completing their case-in-chief by Tuesday morning. So that's the best I can tell you right now in terms of what the government's going to do.

And then counsel for the defense?

MR. BROWNE: Your Honor, I believe there was some discussion between counsel today, and our best estimate is that

closing arguments would be Thursday morning.

THE COURT: Okay.

MR. BROWNE: And the case would be in the jury's hands.

THE COURT: All right. So that's the best projection I can give the jury at this point in time.

And I will remind you, again, same thing I've told you to the point of ad nauseam, don't talk to anybody about the case, don't share any thoughts, don't read anything even on the subject matter of the case. Just stay away from it completely.

It's going to be nice this weekend. Enjoy it. And we'll see you all Monday morning, ready to go at 9:00. Thank you for your service.

(Jury exits the courtroom)

THE COURT: Counsel, I don't expect a line-by-line recitation of what's going to happen next. But just so that I have an idea, counsel for the government, what's your batting order to the completion of trial on Tuesday morning?

MR. WILKINSON: Just a moment, Your Honor.

You'd like to know the witnesses we expect to call, in order?

THE COURT: Yes.

MR. WILKINSON: Okay. We expect to lead off with CJ Saretto, the owner of Broadway Grill, on Monday morning.

THE COURT: Just one second. Okay.

MR. WILKINSON: And then Chris Forsythe, from BECU.
THE COURT: One second. Okay.
MR. WILKINSON: Bob Kerr, from Grand Central Baking.
THE COURT: Just one second. Okay.
MR. WILKINSON: Chris Doyle, from MAD Pizza.
THE COURT: Okay.
MR. WILKINSON: Diane Cole, from Casa Mia.
THE COURT: Okay.
MR. WILKINSON: Mr. Knoernschild, with a "K," who's an individual victim.
THE COURT: Okay.
MR. WILKINSON: Joel Angelastri, from City News Stand.
THE COURT: Okay.
MR. WILKINSON: And if that doesn't fill up our day, we will put on Megan Wood, from the Secret Service. And there may be minor adjustments within that order, depending on witness convenience, but that's what we expect for the day.
THE COURT: And do you -- are there any witnesses on the government's list, at this point, that you do not expect to call?
MR. WILKINSON: Yes. And I should say, also, that we are planning to -- we're still working out when Mr. Bussing, from Red Pepper Pizza, will come. He's also a possibility for Monday. If not, then he would be Tuesday.

So witnesses who are off are Tim Chen; Jay Field, who's Number 9. Ruth Gebhard is 99 percent we're not calling her. We expect not to call Mr. Geiger as part of our case-in-chief, though he may testify as a rebuttal expert. Detective Chris Hansen will not be testifying. Special Agent Brad Leopard will not be testifying. And I think that covers it.

THE COURT: Okay. All right. And assuming you finish on Tuesday morning, counsel for the defense?

MS. SCANLAN: Yes, Your Honor. Mr. Blank is scheduled to be here Tuesday morning.

THE COURT: Okay. And Mr. Blank's traveling from out of town?

MS. SCANLAN: Mt. Vernon.

THE COURT: Okay. All right. And any projections on the amount of time necessary for Mr. Blank's testimony?

MS. SCANLAN: I'd say half a day, altogether. I don't think he's going to be up there for that long.

THE COURT: Okay. What I'm trying to do is trying to get jury instructions to you so that you can work on those.

And it looks like we should be able to finish the case, on both sides, sometime on Wednesday?

MR. WILKINSON: Yes.

THE COURT: And the lawyers, apparently, had a discussion about doing closing on Thursday?

MS. SCANLAN: If I may, I think we're 99 percent sure

that Ovie Carroll is coming in rebuttal to Mr. Blank, which would fill up the rest of Wednesday.

THE COURT: Okay. And --

MR. WILKINSON: Your Honor, from our perspective, we actually think it's reasonably possible that we could get Mr. Carroll off on Wednesday morning, which, you know, if people were inclined to speed things along, would allow for closings on Wednesday. So we still see that as a possibility.

THE COURT: I'm flexible. I'll try and get the jury instructions to you so that we can take exceptions at a break, or any opportunity that we have to deal with that, maybe keep you late one day, just so that we can get that out, and not have to burden the jury while we wrestle with that. I don't like to have the jury wait while we wrestle through the jury instructions. That's not my practice.

Anything else to take up, from the government?

MR. WILKINSON: No, Your Honor.

THE COURT: Defense?

MR. BARBOSA: No, Your Honor.

MS. SCANLAN: If I may just request that if we're going to stay late one day, if we could identify that day as soon as you know, I would appreciate it.

THE COURT: I don't know yet myself, Counsel. As soon as I know, I certainly will share it with you.

MS. SCANLAN: Thank you.

THE COURT: All right. Have a good weekend, everybody.

(Adjourned)

(End of requested transcript)

* * *

I certify that the foregoing is a correct transcript from the record of proceedings in the above matter.

Date: 8/19/16 /s/ Andrea Ramirez

Signature of Court Reporter